ENUMERATION OF $\mathrm{AGL}(\frac{m}{3}, \mathbb{F}_{p^3})$-INVARIANT EXTENDED CYCLIC CODES

XIANG-DONG HOU

ABSTRACT. Let p be a prime and let $r,\ e,\ m$ be positive integers such that $r|e$ and $e|m$. The enumeration of linear codes of length p^m over $\mathbb{F}_{p^r}$ which are invariant under the affine linear group $\mathrm{AGL}(\frac{m}{e}, \mathbb{F}_{p^e})$ is equivalent to the enumeration of certain ideals in a partially ordered set $(\mathcal{U}, \prec)$ where $\mathcal{U} = \{0, 1, \cdots, \frac{m}{e}(p-1)\}^e$ and $\prec$ is defined by an e-dimensional simplicial cone. When $e = 2$, the enumeration problem was solved in an earlier paper. In the present paper, we consider the cases $e = 3$. We describe methods for enumerating all $\mathrm{AGL}(\frac{m}{3}, \mathbb{F}_{p^3})$-invariant linear codes of length p^m over $\mathbb{F}_{p^r}$

1. INTRODUCTION

Extended cyclic codes which are invariant under a certain affine linear group were first studied by Kasami, Lin and Peterson [9] and by Delsarte [7]. These codes were further investigated by Charpin [4] [5], by Berger [1], Berger and Charpin [2] [3] in the context of permutation groups, and by Charpin and Levy-Dit-Vehel [6] in conjunction with self-duality. Extended cyclicity follows from affine invariance except when the code is the full ambient space; see later in the introduction. Affine-invariant codes are interesting because of the large automorphism groups they possess. Examples of affine-invariant codes include the q-ary Reed-Muller codes which are precisely $\mathrm{AGL}(m, \mathbb{F}_q)$-invariant codes of length q^m over $\mathbb{F}_q$.

The interest of affine-invariant codes is not limited to coding theory. As we will see below, such codes are precisely submodule of a certain module over the group algebra $\mathbb{K}[\mathrm{AGL}(n, \mathbb{F})]$ where $\mathbb{F}$ and $\mathbb{K}$ are two finite fields of the same characteristic. Therefore, affine-invariant codes provide concrete examples of modular representations of the affine linear group $\mathrm{AGL}(n, \mathbb{F})$.

The present paper and its predecessor [8] deal with the enumeration of affine-invariant codes. Delsarte's characterization of affine–invariant extended cyclic codes in terms of defining sets [7] is the foundation of our work. The starting point of our approach is a reformulation (Theorem 1.1) of Delsarte's characterization; the reformulation changes the enumeration problem from an algebraic one to a combinatorial and geometric one.

A comprehensive introduction to affine-invariant extended cyclic codes can be found in [2]. A detailed introduction to our approach was given in [8]. Thus in the present introduction, we only give the essential facts to be used in the paper.

Let p be a prime and $r,\ m,\ e$ positive integers such that $e|m$. Identify $\mathbb{F}_{p^m}$ with $\mathbb{F}_{p^e}^{m/e}$. Then the affine linear group $\mathrm{AGL}(\frac{m}{e}, \mathbb{F}_{p^e})$ acts on $\mathbb{F}_{p^m}$ hence also acts on

Key words and phrases. affine invariant code, affine linear group, extended cyclic code, partial order, simplicial cone, walk.

the group algebra $\mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)]$. Put

$$G_{m,e} = \mathrm{AGL}(\frac{m}{e}, \mathbb{F}_{p^e}).$$

Then $\mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)]$ is an $\mathbb{F}_{p^r}[G_{m,e}]$-module. Define

$$\mathcal{M} = \Big\{ \sum_{g\in\mathbb{F}_{p^m}} a_g X^g \in \mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)] : \sum_{g\in\mathbb{F}_{p^m}} a_g = 0 \Big\}.$$

$\mathbb{F}_{p^r}[G_{m,e}]$-submodules of $\mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)]$ are *$G_{m,e}$-invariant codes* over $\mathbb{F}_{p^r}$; $\mathbb{F}_{p^r}[G_{m,e}]$-submodules of $\mathcal{M}$ are *$G_{m,e}$-invariant extended cyclic codes* over $\mathbb{F}_{p^r}$. In fact, every proper $\mathbb{F}_{p^r}[G_{m,e}]$-submodules of $\mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)]$ must be contained in $\mathcal{M}$ ([8]).

As pointed out in [8], in order to determine $\mathbb{F}_{p^r}[G_{m,e}]$-submodules of $\mathcal{M}$ for all r, it suffices to determine those with $r|e$. Thus we always assume $r|e$.

Let

$$P = \begin{bmatrix} p^0 & p^{e-1} & \cdots & p^1 \\ p^1 & p^0 & \cdots & p^2 \\ \vdots & \vdots & \ddots & \vdots \\ p^{e-1} & p^{e-2} & \cdots & p^0 \end{bmatrix}.$$

For $u, v \in \mathbb{R}^e$, we say $u \prec v$ if $(u-v)P$ has all the coordinates ≤ 0. Let $\Delta \subset \mathbb{R}^e$ be the set of all linear combinations of the rows of

$$(1-p^e)P^{-1} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & -p \\ -p & 1 & 0 & \cdots & 0 & 0 \\ 0 & -p & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & -p & 1 \end{bmatrix}$$

with nonnegative coefficients. Namely, Δ is the e-dimensional simplicial cone spanned by the rows of $(1-p^e)P^{-1}$. It is clear that $u \prec v$ if and only if $u \in v + \Delta$. The relation $\prec$ is a partial order in $\mathbb{R}^e$.

Let

$$A = \begin{bmatrix} 0 & & & & & 1 \\ 1 & 0 & & & & \\ & 1 & 0 & & & \\ & & & \ddots & & \\ & & & & 0 & \\ & & & & 1 & 0 \end{bmatrix}_{e\times e}$$

be the circulant permutation matrix. Since $AP = PA$, the matrix A preserves the partial order $\prec$, i.e., $u \prec v$ if and only if $uA \prec vA$.

For any subset $\Omega \subset \mathbb{R}^e$, $(\Omega, \prec)$ is a partially ordered set. An *ideal* of $(\Omega, \prec)$ is a subset $I \subset \Omega$ such that for each $u \in I$ and $v \in \Omega$, $v \prec u$ implies $v \in I$.

Let

$$\mathcal{U} = \Big\{0, 1, \cdots, \frac{m}{e}(p-1)\Big\}^e.$$

For each $s \in \{0, 1, \cdots, p^m - 1\}$, write

$$s = s_0 p^0 + \cdots + s_{m-1} p^{m-1}, \quad 0 \le s_i \le p-1,$$

and define

$$\sigma(s) = \Big[\sum_{i\equiv 0 \pmod e} s_i, \sum_{i\equiv 1 \pmod e} s_i, \ \ldots, \sum_{i\equiv e-1 \pmod e} s_i \Big] \in \mathcal{U}.$$

The following is a reformulation of Delsarte's characterization of affine-invariant extended cyclic codes [7]:

Theorem 1.1. ([8]) *There is a one-to-one correspondence between the $\mathbb{F}_{p^r}[G_{m,e}]$-submodules of $\mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)]$ and the A^r-invariant ideals of $(\mathcal{U}, \prec)$. If I is an A^r-invariant ideal of $(\mathcal{U}, \prec)$, the corresponding $\mathbb{F}_{p^r}[G_{m,e}]$-submodules of $\mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)]$ is*

$$\begin{aligned} M(I) := \Big\{ \sum_{g\in\mathbb{F}_{p^m}} a_g X^g \in \mathbb{F}_{p^r}[(\mathbb{F}_{p^m}, +)] : \sum_{g\in\mathbb{F}_{p^m}} a_g g^s = 0 \\ \text{for all } s \in \{0, 1, \cdots, p^m - 1\} \text{ with } \sigma(s) \in I \Big\}. \end{aligned} \tag{1.1}$$

In (1.1), 0^0 *is defined as* 1. *Moreover, $M(I) \subset \mathcal{M}$ if and only if $I \neq \emptyset$.*

Note. When $e = m$, i.e., when $\mathcal{U} = \{0, 1, \ldots, p-1\}^e$, the partial order $\prec$ in $\mathcal{U}$ is the cartesian product of linear orders. Namely, $(x_1, \ldots, x_e) \prec (y_1, \ldots, y_e)$ in $\mathcal{U}$ if and only if $x_i \leq y_i$ for all $1 \leq i \leq e$. However, this is not the case when $1 < e < m$.

Example 1.2. Let $p = 3$, $m = 6$, $e = 3$, $r = 1$ and

$$\begin{aligned} I = \big\{ &(0,0,0),\ (1,0,0),\ (0,1,0),\ (0,0,1), \\ &(0,1,1),\ (1,0,1),\ (1,1,0),\ (1,1,1), \\ &(2,0,0),\ (0,2,0),\ (0,0,2), \\ &(3,0,0),\ (0,3,0),\ (0,0,3) \big\}. \end{aligned}$$

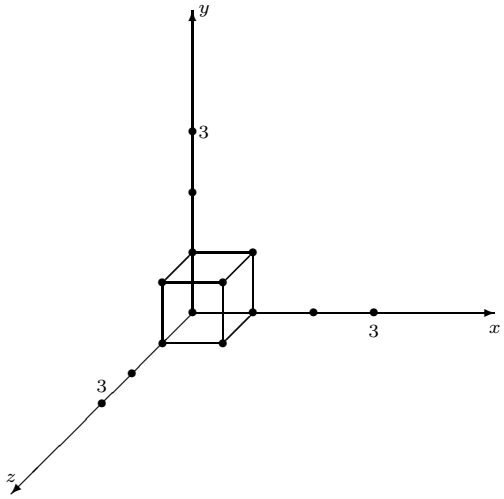

Figure 1. The A-invariant ideal I

It is easy to see that I is an A-invariant ideal of $(\mathcal{U}, \prec)$. We have

$$\begin{aligned}\sigma^{-1}(I) = \big\{&0,\ 1,\ 2,\ 3,\ 4,\ 6,\ 9,\ 10,\ 12,\ 13,\ 18,\ 27,\ 28,\ 29,\ 30,\ 36,\ 39,\ 54,\\ &55,\ 81,\ 82,\ 84,\ 87,\ 90,\ 91,\ 108,\ 117,\ 162,\ 165,\ 243,\ 244,\\ &246,\ 247,\ 252,\ 261,\ 270,\ 273,\ 324,\ 325,\ 351,\ 486,\ 495\big\}.\end{aligned}$$

The $\mathbb{F}_3[G_{6,3}]$-submodule of $\mathcal{M}$ corresponding to I is

$$M(I) = \Big\{ \sum_{g\in\mathbb{F}_{3^6}} a_g X^g \in \mathbb{F}_3[(\mathbb{F}_{3^6}, +)] : \sum_{g\in\mathbb{F}_{3^6}} a_g g^s = 0 \text{ for all } s \in \sigma^{-1}(I)\Big\}.$$

Therefore, the essential problem is how to enumerate the A^r-invariant ideals of $(\mathcal{U}, \prec)$. When $e = 1$, the problem is trivial. When $e = 2$, the problem has been solved in [8]. The present paper deals with the case $e = 3$. We will describe methods for enumerating all A^r-invariant ideals of $(\mathcal{U}, \prec)$ for $e = 3$.

2. Description of the Approach

For simplicity, an ideal of $(\Omega, \prec)$, where $\Omega \subset \mathbb{R}^e$, is called an ideal of Ω.

Lemma 2.1. (i) *Let $\Omega \subset \Gamma \subset \mathbb{R}^e$ such that Ω and Γ are A^r-invariant. If I is an A^r-invariant ideal of Ω, then there is an A^r-invariant ideal J of Γ such that $J \cap \Omega = I$.*

(ii) *Let $\Omega \subset \mathbb{R}^e$ and $\Gamma \subset \mathbb{R}^e$. Let I be an ideal of Ω and J an ideal of Γ such that $I \cap \Gamma = J \cap \Omega$. Then $I \cup J$ is an ideal of $\Omega \cup \Gamma$ if and only if*

$$(I + \Delta) \cap \Gamma \subset J \quad \text{and} \quad (J + \Delta) \cap \Omega \subset I. \tag{2.1}$$

Proof. (i) Let $J = (I + \Delta) \cap \Gamma$. Then J is an A^r-invariant ideal of Γ. Since I is an ideal of Ω, we have $J \cap \Omega = (I + \Delta) \cap \Omega = I$.

(ii) ($\Rightarrow$) Since $(I + \Delta) \cap (\Omega \cup \Gamma)$ is the ideal of $\Omega \cup \Gamma$ generated by I, i.e., the smallest ideal of $\Omega \cup \Gamma$ containing I, and since $I \cup J$ is an ideal of $\Omega \cup \Gamma$, we have $(I + \Delta) \cap (\Omega \cup \Gamma) \subset I \cup J$. Hence

$$\begin{aligned}(I + \Delta) \cap \Gamma &= (I + \Delta) \cap (\Omega \cup \Gamma) \cap \Gamma\\ &\subset (I \cup J) \cap \Gamma\\ &= (I \cap \Gamma) \cup J\\ &= (J \cap \Omega) \cup J\\ &= J.\end{aligned}$$

In the same way, $(J + \Delta) \cap \Omega \subset I$.

($\Leftarrow$) We have

$$(I + \Delta) \cap (\Omega \cup \Gamma) = \big[(I + \Delta) \cap \Omega\big] \cup \big[(I + \Delta) \cap \Gamma\big] \subset I \cup J$$

since $(I + \Delta) \cap \Omega = I$ and, by (2.1), $(I + \Delta) \cap \Gamma \subset J$. In the same way, $(J + \Delta) \cap (\Omega \cup \Gamma) \subset I \cup J$. Therefore,

$$\big[(I \cup J) + \Delta\big] \cap (\Omega \cup \Gamma) \subset I \cup J,$$

which makes $I \cup J$ an ideal of $\Omega \cup \Gamma$. □

In general, all A^r-invariant ideals of $\mathcal{U}$ can be constructed using the following inductive strategy. Partition $\mathcal{U}$ into A^r-invariant subsets $\mathcal{U}_1, \ldots, \mathcal{U}_k$. Let $1 \le i \le k$ and assume that for each j with $j < i$, an A^r-invariant ideal I_j of $\mathcal{U}_j$ has been

constructed such that $\bigcup_{j<i} I_j$ is an ideal of $\bigcup_{j<i} \mathcal{U}_j$. Construct an A^r-invariant ideal I_i of $\mathcal{U}_i$ such that for all $j < i$,

$$(I_i + \Delta) \cap \mathcal{U}_j \subset I_j \quad \text{and} \quad (I_j + \Delta) \cap \mathcal{U}_i \subset I_i. \tag{2.2}$$

Then by Lemma 2.1 (ii), $\bigcup_{j\le i} I_j$ is an A^r-invariant ideal of $\bigcup_{j\le i} \mathcal{U}_j$. Eventually, $I = \bigcup_{j\le k} \mathcal{U}_j$ is an A^r-invariant ideal of $\mathcal{U}$ with $I \cap \mathcal{U}_i = I_i$ for all $1 \le i \le k$. We shall call an ideal I_i of $\mathcal{U}_i$ satisfying (2.2) *compatible* with I_j $(j < i)$.

Remarks. (i) Constructing an A^r-invariant ideal I in $\mathcal{U}$ is an e-dimensional geometric problem. By partitioning $\mathcal{U}$ suitably, constructing an A^r-invariant ideal I_i in $\mathcal{U}_i$ becomes an $(e-1)$-dimensional geometric problem.

(ii) Since for each A^r-invariant ideal I of $\mathcal{U}$, $I \cap \mathcal{U}_i$ $(1 \le i \le k)$ is A^r-invariant ideal of $\mathcal{U}_i$, the above strategy does enumerate all A^r-invariant ideals of $\mathcal{U}$.

(iii) The existence of an A^r-invariant ideal I_i of $\mathcal{U}_i$ compatible with I_j $(j < i)$ is guaranteed by Lemma 2.1. Hence the inductive construction can always be completed.

To turn the above strategy into an enumeration algorithm, what we essentially need are effective methods for enumerating all A^r-invariant ideals I_i which are compatible with an existing sequence of A^r-invariant ideals I_j $(j < i)$. The main purpose of this paper is to provide such effective methods in the case $e = 3$.

Form now on, we assume $e = 3$. Put

$$n = \frac{m}{3}(p-1).$$

Since $r|e$, there are two possibilities for r: $r = 1$ or 3. When $r = 3$, we partition $\mathcal{U}$ as

$$\mathcal{U} = \bigcup_{i=0}^{n} \mathcal{U}_i \tag{2.3}$$

where

$$\mathcal{U}_i = \big\{(x, y, z) \in \mathcal{U} : z = i\big\}.$$

When $r = 1$, we partition $\mathcal{U}$ as

$$\mathcal{U} = \bigcup_{i=0}^{n} \mathcal{V}_i \tag{2.4}$$

where

$$\mathcal{V}_i = \big\{(x, y, z) \in \mathcal{U} : x \le i,\ y \le i,\ z \le i,\ \text{and at least one of } x, y, z \text{ is } i\big\}.$$

Section 4 deals with the case $r = 3$. We describe two methods for enumerating compatible ideals I_i of $\mathcal{U}_i$. The method of forward slicing enumerates all ideals I_i of $\mathcal{U}_i$ which are compatible with ideals I_j of $\mathcal{U}_j$ where $0 \le j < i$; the method of backward slicing enumerates all ideals I_i of $\mathcal{U}_i$ which are compatible with ideals I_j of $\mathcal{U}_j$ where $i < j \le n$. Section 5 deals with the case $r = 1$. We describe a method for enumerating all A-invariant ideals I_i of $\mathcal{V}_i$ compatible with A-invariant ideals I_j of $\mathcal{V}_j$ where $0 \le j < i$. In preparation for these attempts, in the next section, we first take a close look of the cross section of an ideal in $\mathcal{U}$ on a plane parallel to a coordinate plane. We also introduce the notion of walk in the next section.

3. Cross Sections and Walks

Let $c \in \mathbb{R}$. Observe that $\Delta \cap (\mathbb{R}^2 \times \{c\})$ consists of points $(x, y, c) \in \mathbb{R}^3$ satisfying

$$\begin{cases} x + py + p^2 c \le 0, \\ p^2 x + y + pc \le 0, \\ px + p^2 y + c \le 0, \end{cases}$$

i.e.,

$$\begin{cases} x + py \le \min\{-p^2 c,\ -\frac{1}{p} c\}, \\ p^2 x + y \le -pc. \end{cases} \tag{3.1}$$

The solution set of (3.1) is depicted in Figure 2 when $c \ge 0$ and in Figure 3 when $c < 0$.

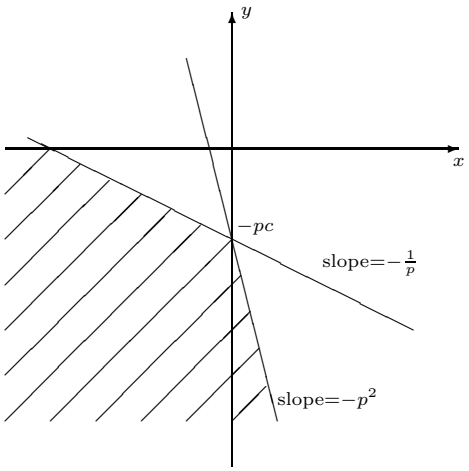

Figure 2. The cross section of Δ on the plane $z = c$, $c \ge 0$

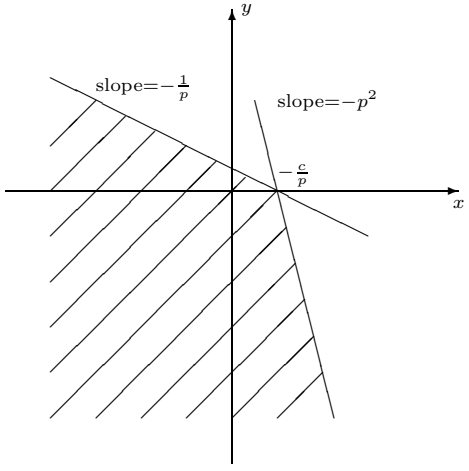

Figure 3. The cross section of Δ on the plane $z = c$, $c < 0$

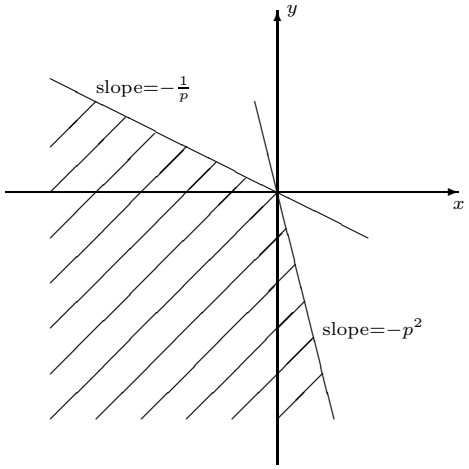

Figure 4. The region D

Let

$$D = \big\{(x,y) \in \mathbb{R}^2 : x + py \le 0,\ p^2x + y \le 0\big\}$$

(Figure 4). We can write

$$\Delta \cap (\mathbb{R}^2 \times \{c\}) = \begin{cases} \big(D - c(0,p)\big) \times \{c\}, & \text{if } c \ge 0, \\ \big(D - c(\frac{1}{p},0)\big) \times \{c\}, & \text{if } c < 0. \end{cases} \tag{3.2}$$

Given (x_1,y_1,z_1) and (x_2,y_2,z_2) in $\mathbb{R}^3$, $(x_1,y_1,z_1) \prec (x_2,y_2,z_2)$ if and only if $(x_1,y_1,z_1) - (x_2,y_2,z_2) \in \Delta \cap \big(\mathbb{R}^2 \times \{z_1 - z_2\}\big)$. By (3.2), this happens if and only if

$$(x_1,y_1) \in (x_2,y_2) + \begin{cases} D - (z_1 - z_2)(0,p), & \text{if } z_1 \ge z_2, \\ D - (z_1 - z_2)(\frac{1}{p},0), & \text{if } z_1 < z_2. \end{cases} \tag{3.3}$$

Thus

$$\begin{aligned} &\big[(x_2,y_2,z_2) + \Delta\big] \cap \big[\mathbb{R}^2 \times \{z_1\}\big] \\ &= \begin{cases} \big[(x_2,y_2) + D - (z_1 - z_2)(0,p)\big] \times \{z_1\}, & \text{if } z_1 \ge z_2, \\ \big[(x_2,y_2) + D - (z_1 - z_2)(\frac{1}{p},0)\big] \times \{z_1\}, & \text{if } z_1 < z_2. \end{cases} \end{aligned} \tag{3.4}$$

By symmetry, we also see that $(x_1,y_1,z_1) \prec (x_2,y_2,z_2)$ if and only if

$$(y_1,z_1) \in (y_2,z_2) + \begin{cases} D - (x_1 - x_2)(0,p), & \text{if } x_1 \ge x_2, \\ D - (x_1 - x_2)(\frac{1}{p},0), & \text{if } x_1 < x_2, \end{cases} \tag{3.5}$$

which is equivalent to

$$(z_1,x_1) \in (z_2,x_2) + \begin{cases} D - (y_1 - y_2)(0,p), & \text{if } y_1 \ge y_2, \\ D - (y_1 - y_2)(\frac{1}{p},0), & \text{if } y_1 < y_2. \end{cases} \tag{3.6}$$

Lemma 3.1. *Let c be an integer written in the form $c = ap + b$ where $a, b \in \mathbb{Z}$, $0 \le b \le p-1$. Then*

$$\Big[c(\frac{1}{p},0) + D\Big] \cap \mathbb{Z}^2 = \Big[\big\{(a,0),\ (a+1, -p^2 + pb)\big\} + D\Big] \cap \mathbb{Z}^2.$$

Proof. Note that

$$\Big[c(\frac{1}{p},0)+D\Big]\setminus\Big[\big\{(a,0),\ (a+1,-p^2+pb)\big\}+D\Big]$$

is the indicated region in Figure 5. Obvious, this region does not contain any points in $\mathbb{Z}^2$ □

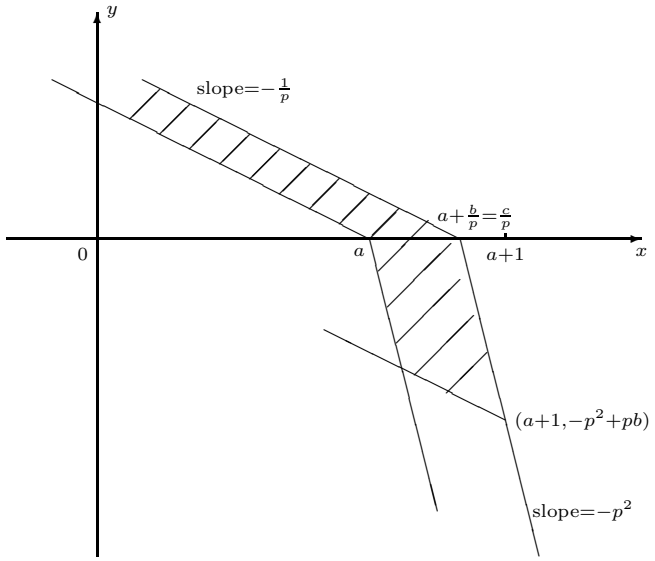

Figure 5. Proof of Lemma 3.1

The restriction of $\prec$ on the xy-plane, still denoted by $\prec$, is defined by the 2-dimensional cone D: $(x_1,y_1)\prec(x_2,y_2)$ if and only if $(x_1,y_1)\prec(x_2,y_2)+D$. It is clear that for $I\subset\Omega\subset\mathbb{R}^2$ and $c\in\mathbb{R}$, $I\times\{c\}$ is an ideal of $\Omega\times\{c\}$ if and only if I is an ideal of Ω.

For integers $a\le b$, let

$$[a,b]=\{x\in\mathbb{Z}:a\le x\le b\}.$$

Following the approach in [8], we can characterize ideals of a rectangle in $\mathbb{Z}^2$ by their boundaries. Such boundaries are called walks.

Definition 3.2. Let $a\le b$ and $c\le d$ be integers. A *walk* in $[a,b]\times[c,d]$ is a sequence

$$(x_0,y_0),\ (x_1,y_1),\ \ldots,\ (x_k,y_k) \tag{3.7}$$

in $[a,b]\times[c,d]$ satisfying the following conditions.

(i) $x_0=a$ or $y_0=d$; $x_k=b$ or $y_k=c$.
(ii) For each $0<i\le k$, either $(x_i,y_i)=(x_{i-1}+h,\ y_{i-1})$ for some $1\le h\le p$ or $(x_i,y_i)=(x_{i-1},\ y_{i-1}-v)$ for some $1\le v\le p^2$. In the first case, $\big((x_{i-1},y_{i-1}),\ (x_i,y_i)\big)$ is called a *horizontal step of length* h; in the second case, $\big((x_{i-1},y_{i-1}),\ (x_i,y_i)\big)$ is called a *vertical step of length* v.
(iii) The steps in the sequence (3.7) alternate between horizontal and vertical.

(iv) If $a \le x_0 < b$ and $y_0 = d$, the first step is vertical; if $x_k = b$ and $c \le y_k < d$, the last step in horizontal.
(v) If the first step is horizontal of length h, then $1 \le h \le p-1$; if the last step is vertical of length v, then $1 \le v \le p^2 - 1$

Let $U = [a, b] \times [c, d]$. For each walk $W = \big((x_0, y_0), \ldots, (x_k, y_k)\big)$ in U, denote by $\iota_U(W)$ the lower left part of U bounded by W (see Figure 6), i.e.,

$$\iota_U(W) = \big\{(x, y) \in U : x \le x_i \text{ and } y \le y_i \text{ for some } 0 \le i \le k\big\}.$$

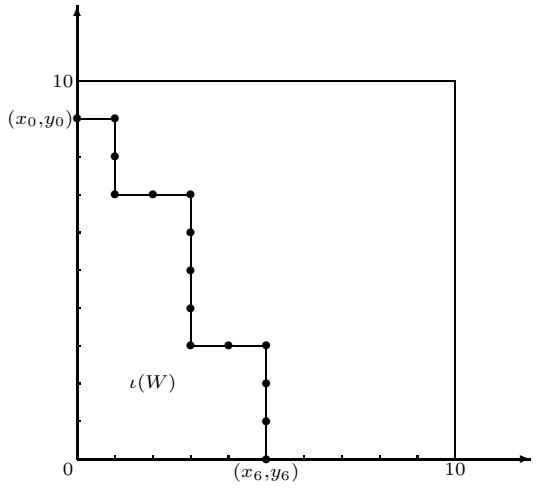

Figure 6. A walk W in $[0, 10] \times [0, 10]$ and its corresponding ideal $\iota(W)$, $p = 2$

We denote the empty walk in U by $\emptyset$ and define $\iota_U(\emptyset) = \emptyset$. Then

$$W \longmapsto \iota_U(W)$$

is a bijection from the set $\mathcal{W}_U$ of all walks in U to the set $\mathcal{I}_U$ of all ideals of U. In fact, the conditions in Definition 3.2 are necessary and sufficient to ensure that for every $u \in \iota_U(W)$, $(u + D) \cap U \subset \iota_U(W)$. The inverse map $\iota_U^{-1} : \mathcal{I}_U \to \mathcal{W}_U$ is denoted by ω_U. When U is clear from the context, ι_U and ω_U are simply written as ι and ω. We call a walk W the *boundary* of the ideal $\iota(W)$ and $\iota(W)$ the *ideal bounded by* W. We remind the reader that the *boundary* here is unrelated to the *border* in [2]

For two walks $W_1,\ W_2 \in \mathcal{W}_U$, we say that $W_1 \le W_2$ if $\iota(W_1) \subset \iota(W_2)$, which simply means that W_1 is below and to the left of W_2. The partially ordered set $(\mathcal{I}_U, \subset)$ is a lattice where "$\wedge$" is "$\cap$" and "$\vee$" is "$\cup$". Consequently, $(\mathcal{W}_U, \le)$ is also a lattice with

$$W_1 \wedge W_2 = \omega\big(\iota(W_1) \cap \iota(W_2)\big)$$

and

$$W_1 \vee W_2 = \omega\big(\iota(W_1) \cup \iota(W_2)\big).$$

We introduce some operations on walks. Let $U_i = [a_i, b_i] \times [c_i, d_i]$ $(i = 1, 2)$, where $a_i \le b_i$ and $c_i \le d_i$ are integers, and assume $U_1 \supset U_2$. Let W be a walk in

U_1 and let $I = \iota_{U_1}(W)$. The *restriction* of W in U_2, denoted by $W|_{U_2}$, is defined to be $\omega_{U_2}(I \cap U_2)$. If $U_2 \subset \iota_{U_1}(W)$, $W|_{U_2}$ is the point (b_2, d_2); otherwise, $W|_{U_2}$ is the walk in U_2 consisting of steps and partial steps of W. (See Figure 7.)

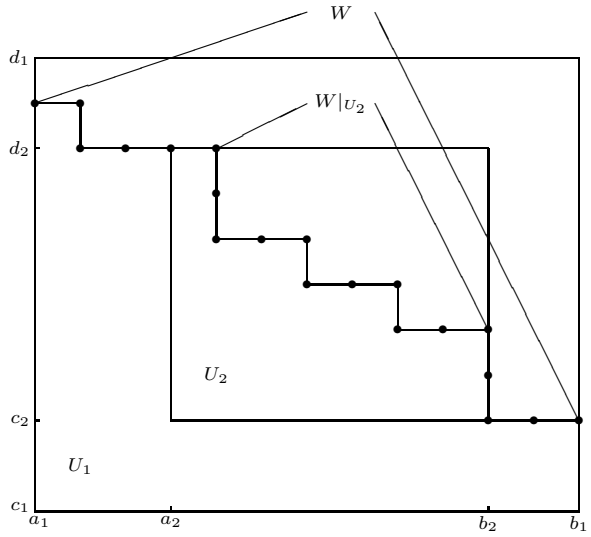

Figure 7. The restriction of a walk

For $h,\ v \in \mathbb{Z}$, the shift of W by h horizontal units and v vertical units is a walk in $[a_1 + h, b_1 + h] \times [c_1 + v, d_1 + v]$ and is denoted by $W + (h, v)$.

Let Z be a walk in U_2 and let $J = \iota_{U_2}(Z)$. A walk W in U_1 is called an *extension* of Z if $W|_{U_2} = Z$. Let $\overline{Z}_{U_1}$ and $\underline{Z}_{U_1}$ be the *highest* and *lowest* (the largest and lowest with respect to $\leq$) extensions of Z in U_1 respectively. Then $\overline{Z}_{U_1} = \omega_{U_1}(K)$ where K is the largest ideal of U_1 such that $K \cap U_2 = J$ and $\underline{Z}_{U_1} = \omega_{U_1}(L)$ where L is the smallest ideal of U_1 such that $L \cap U_2 = J$. In fact, $\underline{Z}_{U_1}$ is the boundary of $(J + D) \cap U_1$. $\overline{Z}_{U_1}$ can be obtained from Z easily: If Z is the point (b_2, d_2) (i.e., $J = U_2$), $\overline{Z}_{U_1}$ is the point (b_1, d_1). If Z is not the point (b_2, d_2) and $Z \neq \emptyset$, we extend Z to the lower right with steps alternating between horizontal ones of largest possible lengths and vertical ones of length 1, and to the upper left with steps alternating between vertical ones of largest possible lengths and horizontal ones of length 1. If $Z = \emptyset$ and $(a_1, b_1) \neq (a_2, b_2)$, we start from the point $\big(\max\{a_2 - 1, a_1\}, \max\{b_2 - 1, b_1\}\big)$ and extend to the lower right and to the upper left as described above. (See Figure 8.) If $Z = \emptyset$ and $(a_1, b_1) = (a_2, b_2)$, then $\overline{Z}_{U_1} = \emptyset$. $\underline{Z}_{U_1}$ is obtained in a similar way. (See Figure 9.)

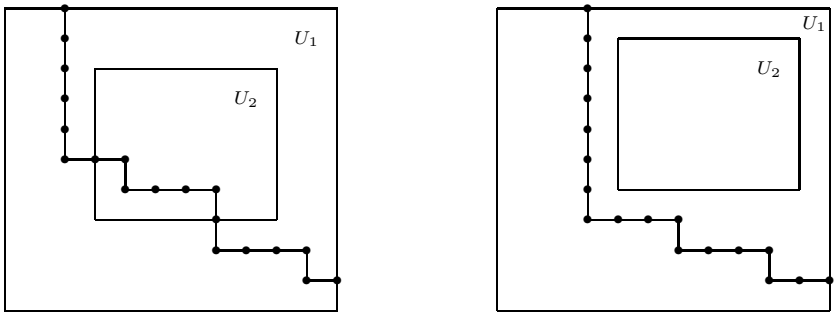

Figure 8. Examples of highest extensions, $p = 3$

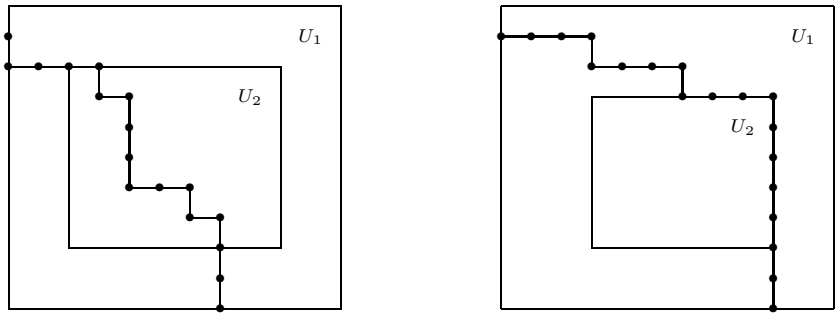

Figure 9. Examples of lowest extensions, $p = 3$

We list some obvious properties of restrictions and extensions. Let U_i, $i = 1, 2, 3$, be rectangles in $\mathbb{Z}^2$ such that $U_1 \supset U_2 \supset U_3$. Let W be a walk in U_1 and Z a walk in U_3. We have

$$\begin{gathered}(W|_{U_2})|_{U_3} = W|_{U_3},\\ \overline{(\overline{Z}_{U_2})}_{U_1} = \overline{Z}_{U_1},\\ \underline{(\underline{Z}_{U_2})}_{U_1} = \underline{Z}_{U_1},\\ (\overline{Z}_{U_2})|_{U_3} = (\underline{Z}_{U_2})|_{U_3} = Z.\end{gathered}$$

4. Enumerating Ideals of $\mathcal{U}$

In this section we assume $r = 3$. Since A^3 is the identity matrix, A^3-invariant ideals of $\mathcal{U}$ are simply ideals of $\mathcal{U}$. Recall that $n = \frac{m}{3}(p-1)$. Put

$$U = [0, n]^2,$$

and partition $\mathcal{U}$ as

$$\mathcal{U} = \bigcup_{i=0}^{n} (U \times \{i\}).$$

A sequence of ideals $J_0, \ldots, J_{i-1}$ (or $J_{i+1}, \ldots, J_n$) of U is called *forward* (respectively, *backward*) *consistent* if $\bigcup_{j=0}^{i-1}(J_j \times \{j\})$ is an ideal of $U \times [0, i-1]$ (respectively, $\bigcup_{j=i+1}^{n}(J_j \times \{j\})$ is an ideal of $U \times [i+1, n]$). An ideal J_i of U is said to be *consistent*

with $J_0, \dots, J_{i-1}$ (or $J_{i+1}, \dots, J_n$) if $J_0, \dots, J_{i-1}, J_i$ (respectively, $J_i, J_{i+1}, \dots, J_n$) is forward (backward) consistent.

Note. In the terminology of Section 2, the statement that J_i is *consistent* with $J_0, \dots, J_{i-1}$ means that $J_i \times \{i\}$ is *compatible* with $J_j \times \{j\}$, $0 \le j < i$, with respect to the partition $\mathcal{U} = \bigcup_{j=0}^{n}(U \times \{j\})$. The meaning of the statement that J_i is *consistent* with $J_{i+1}, \dots, J_n$ is similar.

Given a forward consistent sequence of ideals $J_0, \dots, J_{i-1}$ (or a backward consistent sequence $J_{i+1}, \dots, J_n$), our goal in this section is to enumerate all ideals J_i of U which are consistent with $J_0, \dots, J_{i-1}$ (or $J_{i+1}, \dots, J_n$). When $n < p$, the problem is trivial: In this case, the partial order $\prec$ in $\mathcal{U}$ is the cartesian product of linear orders, hence J_i is consistent with $J_0, \dots, J_{i-1}$ (or $J_{i+1}, \dots, J_n$) if and only if $J_i \subset J_{i-1}$ (or $J_i \supset J_{i+1}$.) When $n \ge p$, the problem is more complex. The main result of this section is the determination of two walks X_i and Y_i in U, which can be computed from the boundaries of $J_0, \dots, J_{i-1}$ (respectively, the boundaries of $J_{i+1}, \dots, J_n$), such that J_i is consistent with $J_0, \dots, J_{i-1}$ (or $J_{i+1}, \dots, J_n$) if and only if $X_i \le \omega(J_i) \le Y_i$.

Lemma 4.1. *Let i be an integer with $0 \le i \le n$ and let J_i be an ideal of U.*

(i) *Let $J_0, \dots, J_{i-1}$ be a forward consistent sequence of ideals of U. Then J_i is consistent with $J_0, \dots, J_{i-1}$ if and only if*

$$\big[J_j + D - (i-j)(0,p)\big] \cap U \subset J_i, \quad 0 \le j < i \tag{4.1}$$

and

$$\big[J_i + D + (a,0)\big] \cap U \subset J_{i-ap-b}, \tag{4.2}$$

$$\big[J_i + D + (a+1, -p^2+pb)\big] \cap U \subset J_{i-ap-b} \tag{4.3}$$

for all $a, b \in \mathbb{Z}$ with $a \ge 0$, $0 \le b \le p-1$, $ap + b \le i$.

(ii) *Let $J_{i+1}, \dots, J_n$ be a backward consistent sequence of ideals of U. Then J_i is consistent with $J_{i+1}, \dots, J_n$ if and only if*

$$\big[J_i + D - (j-i)(0,p)\big] \cap U \subset J_j, \quad i < j \le n \tag{4.4}$$

and

$$\big[J_{i+ap+b} + D + (a,0)\big] \cap U \subset J_i, \tag{4.5}$$

$$\big[J_{i+ap+b} + D + (a+1, -p^2+pb)\big] \cap U \subset J_i \tag{4.6}$$

for all $a, b \in \mathbb{Z}$ with $a \ge 0$, $0 \le b \le p-1$, $i + ap + b \le n$.

Proof. (i) By Lemma 2.1 (ii), J_i is consistent with $J_0, \dots, J_{i-1}$ if and only if for every $0 \le j < i$,

$$\big(J_j \times \{j\} + \Delta\big) \cap \big(U \times \{i\}\big) \subset J_i \times \{i\} \tag{4.7}$$

and

$$\big(J_i \times \{i\} + \Delta\big) \cap \big(U \times \{j\}\big) \subset J_j \times \{j\}. \tag{4.8}$$

However, by (3.4), we see that (4.7) is equivalent to (4.1) and (4.8) is equivalent to

$$\big[J_i + D + (i-j)(\frac{1}{p}, 0)\big] \cap U \subset J_j. \tag{4.9}$$

By Lemma 3.1, (4.9) is equivalent to (4.2) and (4.3).

The proof of (ii) is essentially the same. □

Lemma 4.2. *Let J and K be ideals of U with boundaries W and Z respectively. Let $a \geq 0$ and $b \geq 0$ be integers and let $\bar{K}$ be the largest ideal of $[0, a+n] \times [-b, n]$ such that $\bar{K} \cap U = K$. Then the following conditions are equivalent.*

(i)

$$\big[J + D + (a, -b)\big] \cap U \subset K. \tag{4.10}$$

(ii)

$$J + (a, -b) \subset \bar{K} \cap \big((a, -b) + U\big). \tag{4.11}$$

(iii)

$$\big[J + D + (a, -b)\big] \cap \big([0, a+n] \times [-b, n]\big) \subset \bar{K}. \tag{4.12}$$

(iv)

$$\big[\underline{(W + (a, -b))}_{[0,a+n]\times[-b,n]}\big] \,\big|_U \leq Z. \tag{4.13}$$

(v)

$$W + (a, -b) \leq \big[\overline{Z}_{[0,a+n]\times[-b,n]}\big] \,\big|_{[a,a+n]\times[-b,-b+n]}\,. \tag{4.14}$$

(vi)

$$\underline{(W + (a, -b))}_{[0,a+n]\times[-b,n]} \leq \overline{Z}_{[0,a+n]\times[-b,n]}. \tag{4.15}$$

Proof. Condition (iv) is a restatement of (i) in terms of boundaries. In fact, $\big[\underline{(W + (a, -b))}_{[0,a+n]\times[-b,n]}\big] \,\big|_U$ is the boundary of $\big[J+D+(a, -b)\big]\cap U$. In the same way, (ii) $\Leftrightarrow$ (v) and (iii) $\Leftrightarrow$ (vi). Condition (vi) follows from (iv) through the operation $\overline{\ }_{[0,a+n]\times[-b,n]}$; condition (iv) follows from (vi) through the operation $(\ )|_U$. Similarly, (v) $\Leftrightarrow$ (vi) through operations $\underline{\ }_{[0,a+n]\times[-b,n]}$ and $(\ )|_{[a,a+n]\times[-b,-b+n]}$. □

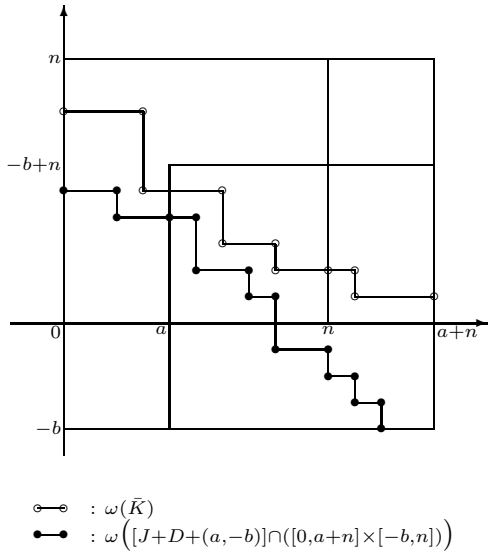

Figure 10. Illustration of Lemma 4.2

Lemma 4.3. *Let J, K, L be ideals of U and let b, c be positive integers. If*

$$\big[J + D + (0, -b)\big] \cap U \subset K \tag{4.16}$$

and

$$\big[K + D + (0, -c)\big] \cap U \subset L, \tag{4.17}$$

then

$$\big[J + D + (0, -b - c)\big] \cap U \subset L \tag{4.18}$$

Proof. Let $\bar{K}$ be the largest ideal of $[0, n] \times [-b - c, -c + n]$ such that

$$\bar{K} \cap \big([0, n] \times [-c, -c + n]\big) = K + (0, -c). \tag{4.19}$$

Then by (4.16) and Lemma 4.2,

$$J + (0, -b - c) \subset \bar{K} \cap \big([0, n] \times [-b - c, -b - c + n]\big). \tag{4.20}$$

Let $\bar{L}$ be the largest ideal of $[0, n] \times [-b - c, n]$ such that $\bar{L} \cap U = L$. Put $\tilde{L} = \bar{L} \cap \big([0, n] \times [-c, n]\big)$. Clearly, $\tilde{L}$ is the largest ideal of $[0, n] \times [-c, n]$ such that $\tilde{L} \cap U = L$. Thus by (4.17) and Lemma 4.2,

$$K + (0, -c) \subset \tilde{L} \cap \big([0, n] \times [-c, -c + n]\big) = \bar{L} \cap \big([0, n] \times [-c, -c + n]\big). \tag{4.21}$$

Let $\hat{L}$ be the largest ideal of $[0, n] \times [-b - c, -c + n]$ such that

$$\hat{L} \cap \big([0, n] \times [-c, -c + n]\big) = \bar{L} \cap \big([0, n] \times [-c, -c + n]\big). \tag{4.22}$$

We claim that

$$\hat{L} = \bar{L} \cap \big([0, n] \times [-b - c, -c + n]\big). \tag{4.23}$$

In fact, $\omega(\bar{L})$ is the highest extension of $\omega\big(\bar{L} \cap ([0, n] \times [-c, n])\big)$; $\omega(\hat{L})$ is the highest extension of $\omega\big(\bar{L} \cap ([0, n] \times [-c, -c + n])\big)$. Since both extensions follow the same rules (described in the last paragraph of Section 3), the new steps (in $[0, n] \times [-b - c, -c]$) in both extensions are identical. Therefore (4.23) is proved.

Note that $\bar{K}$ is an ideal of $[0, n] \times [-b - c, -c + n]$ and that by (4.19) and (4.21),

$$\bar{K} \cap \big([0, n] \times [-c, -c + n]\big) \subset \bar{L} \cap \big([0, n] \times [-c, -c + n]\big).$$

By the maximality of $\hat{L}$, we have $\bar{K} \subset \hat{L}$. However, (4.23) implies that $\hat{L} \subset \bar{L}$. Thus we have $\bar{K} \subset \bar{L}$. Hence by (4.20), we have

$$J + (0, -b - c) \subset \bar{L} \cap \big([0, n] \times [-b - c, -b - c + n]\big),$$

which, by Lemma 4.2, implies (4.18). □

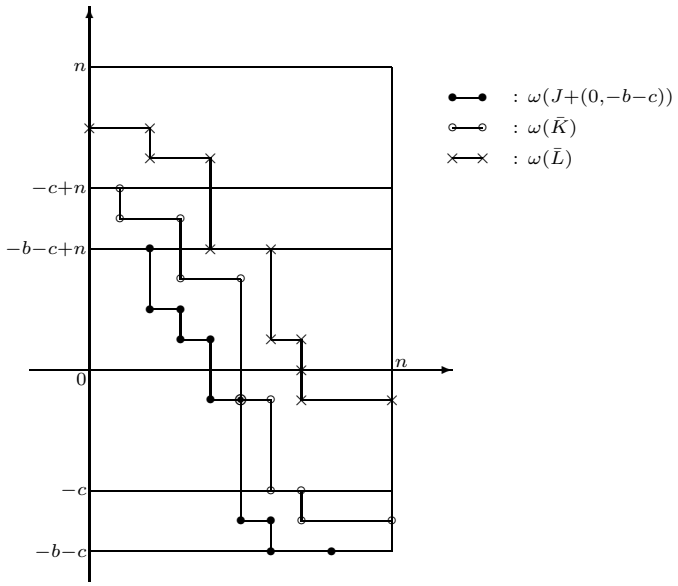

Figure 11. Illustration of Lemma 4.3

Lemma 4.4. *Let J, K, L be ideals of U and let a, b, c, d be nonnegative integers. Assume that*

$$\big[J + D + (a, -b)\big] \cap U \subset K \tag{4.24}$$

and

$$\big[K + D + (c, -d)\big] \cap U \subset L. \tag{4.25}$$

Furthermore, assume that $K \neq \emptyset$, $K \neq U$ and that $\omega(K)$ is not a single horizontal step. (Note that when $n \geq p$, $\omega(K)$ is never a single horizontal step.) Then we have

$$\big[J + D + (a + c, -b - d)\big] \cap U \subset L. \tag{4.26}$$

Proof. Let $\bar{L}$ be the largest ideal of $[0, a + c + n] \times [-b - d, n]$ such that $\bar{L} \cap U = L$ and let $\bar{K}$ be the largest ideal of $[c, a + c + n] \times [-b - d, -d + n]$ such that

$$\bar{K} \cap \big([c, c + n] \times [-d, -d + n]\big) = K + (c, -d).$$

By (4.24) and Lemma 4.2,

$$J + (a + c, -b - d) \subset \bar{K} \cap \big([a + c, a + c + n] \times [-b - d, -b - d + n]\big). \tag{4.27}$$

Put $\tilde{L} = \bar{L} \cap \big([0, c + n] \times [-d, n]\big)$. Clearly, $\tilde{L}$ is the largest ideal of $[0, c + n] \times [-d, n]$ such that

$$\tilde{L} \cap U = L. \tag{4.28}$$

By (4.25) and Lemma 4.2,

$$K + (c, -d) \subset \tilde{L} \cap \big([c, c + n] \times [-d, -d + n]\big). \tag{4.29}$$

Let $\hat{K}$ be the smallest ideal of $[0, c + n] \times [-d, n]$ such that

$$\hat{K} \cap \big([c, c + n] \times [-d, -d + n]\big) = K + (c, -d).$$

By (4.29) and the minimality of $\hat{K}$, we have

$$\hat{K} \subset \tilde{L}. \tag{4.30}$$

The walk $\omega(\hat{K})$ is an extension of $\omega(K+(c,-d))$ to the upper left; the walk $\omega(\bar{K})$ is an extension of $\omega(K+(c,-d))$ to the lower right. (See Figure 12.) Since $K+(c,-d)\neq\emptyset$, $K+(c,-d)\neq[c,c+n]\times[-d,-d+n]$, and since $\omega\big(K+(c,-d)\big)$ is not a single horizontal step, the union (in the obvious sense) of the walks $\omega(\hat{K})$ and $\omega(\bar{K})$ is a walk in $[0,a+c+n]\times[-b-d,-b-d+n]$. Denote this walk by W. Note that

$$\begin{aligned}\iota(W)\cap U &= \hat{K}\cap U\\ &\subset \tilde{L}\cap U \quad \text{(by (4.30))}\\ &= L \quad \text{(by (4.28))}.\end{aligned}$$

Thus by the maximality of $\bar{L}$, we have $\iota(W)\subset\bar{L}$. Hence

$$\begin{aligned}&J+(a+c,-b-d)\\ &\subset \bar{K}\cap\big([a+c,\,a+c+n]\times[-b-d,-b-d+n]\big) \quad \text{(by (4.27))}\\ &= \iota(W)\cap\big([a+c,\,a+c+n]\times[-b-d,-b-d+n]\big)\\ &\subset \bar{L}\cap\big([a+c,\,a+c+n]\times[-b-d,-b-d+n]\big).\end{aligned}$$

By Lemma 4.2, (4.26) follows. □

Remark. If $K=\emptyset$ or $K=U$, or $\omega(K)$ is a single horizontal step, the conclusion in Lemma 4.4 may not be true. Counterexamples are given in Figures 13 – 15.

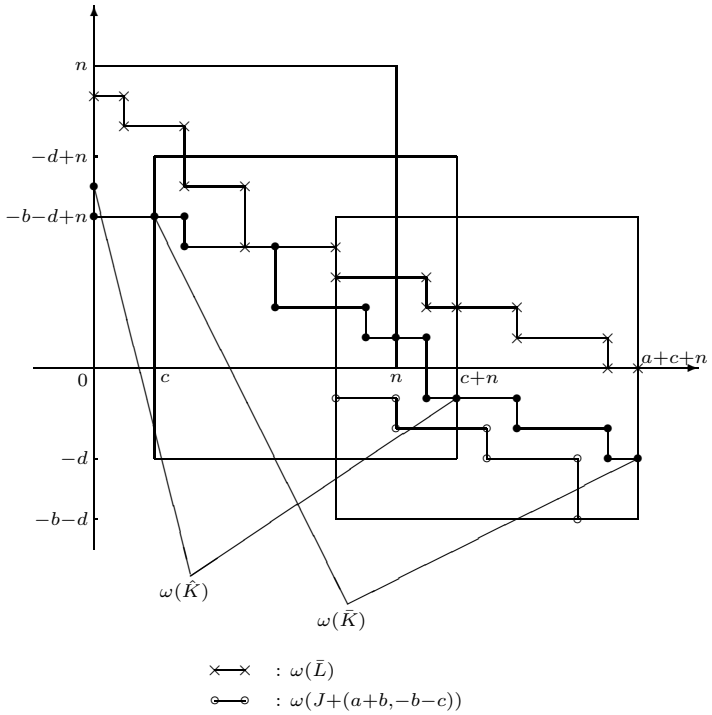

Figure 12. Proof of Lemma 4.4

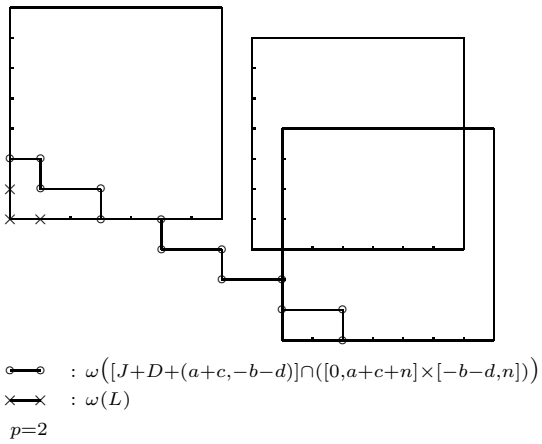

Figure 13. A counterexample of Lemma 4.4: $K = \emptyset$

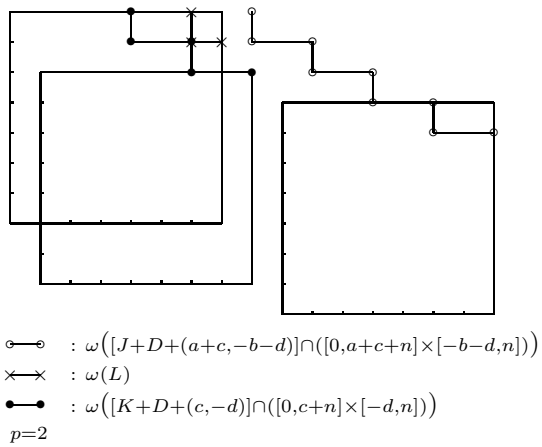

Figure 14. A counterexample of Lemma 4.4: $K = U$

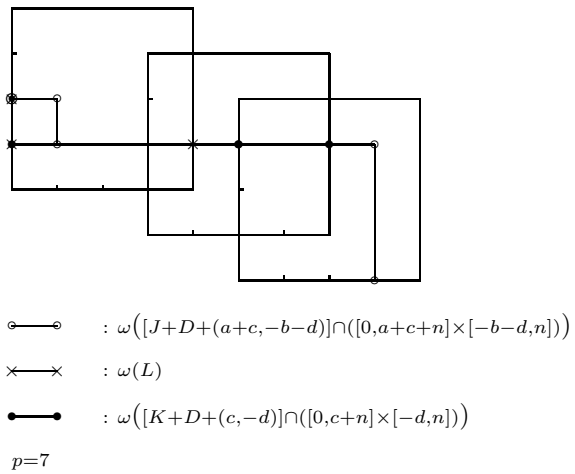

Figure 15. A counterexample of Lemma 4.4: $\omega(K)$ is a single horizontal step

Theorem 4.5. *Let i be an integer with $0 \le i \le n$. Let $J_{i+1}, \dots, J_n$ be a backward consistent sequence of ideals of U and let J_i be an ideal of U. Then J_i is consistent with $J_{i+1}, \dots, J_n$ if and only if the following conditions are satisfied.*

(i) $J_i \supset J_{i+1}$.
(ii) $\big[J_i + D - (0,p)\big] \cap U \subset J_{i+1}$.
(iii) $\big[J_{i+p} + D + (1,0)\big] \cap U \subset J_i$. *(If $i+p > n$, this condition is null.)*
(iv) *Let α_i be the largest integer such that $1 \le \alpha_i \le p-1$, $i+\alpha_i \le n$ and $J_{i+\alpha_i} \ne \emptyset$. Then $\big[J_{i+\alpha_i} + D + (1, -p^2 + p\alpha_i)\big] \cap U \subset J_i$. (If such an α_i does not exist, this condition is null.)*

Proof. First note that the theorem holds when $n < p$. In fact, in this case, since the partial order $\prec$ in $\mathcal{U}$ is the cartesian product of linear orders, J_i is consistent with $J_{i+1}, \dots, J_n$ if and only if (i) is satisfied. Meanwhile, as one can easily see, (ii) is automatically satisfied; (iii) is null; (iv) is either automatically satisfied or is null. Therefore we assume $n \ge p$.

We show that (4.4) – (4.6) in Lemma 4.1 together are equivalent to conditions (i) – (iv) in Theorem 4.5

($\Rightarrow$) Condition (i) follows from (4.5) with $a = 0$ and $b = 1$ since $[J_{i+1} + D] \cap U = J_{i+1}$. Condition (ii) is a special case of (4.4). Conditions (iii) and (iv) are special cases of (4.5) and (4.6).

($\Leftarrow$) To prove (4.4), let $i < j \le n$. By (ii) and the fact that $J_{i+1}, \dots, J_n$ is backward consistent, we have

$$\begin{cases} \big[J_i + D - (0,p)\big] \cap U \subset J_{i+1}, \\ \big[J_{i+1} + D - (j-i-1)(0,p)\big] \cap U \subset J_j, \end{cases}$$

Thus by Lemma 4.3,

$$\big[J_i + D - (j-i)(0,p)\big] \cap U \subset J_j.$$

To prove (4.5), let $a, b \in \mathbb{Z}$ with $a \ge 0$, $0 \le b \le p-1$, $i + ap + b \le n$. We may assume $a \ge 1$ since (4.5) becomes obvious when $a = 0$. By (iii) and the fact that

$J_{i+1}, \ldots, J_n$ is backward consistent, we have

$$\begin{cases} \big[J_{i+p} + D + (1,0)\big] \cap U \subset J_i, \\ \big[J_{i+ap} + D + (a-1,0)\big] \cap U \subset J_{i+p}. \end{cases} \tag{4.31}$$

We claim that

$$\big[J_{i+ap} + D + (a,0)\big] \cap U \subset J_i. \tag{4.32}$$

In fact, if $J_{i+p} \neq \emptyset$ and $J_{i+p} \neq U$, then (4.32) follows from (4.31) and Lemma 4.4. If $J_{i+p} = \emptyset$, then by (i), $J_{i+ap} = \emptyset$ since $J_{i+1}, \ldots, J_n$ is backward consistent. Thus (4.32) holds. If $J_{i+p} = U$, by (i), we have $J_i = U$ and (4.32) also holds. Since $J_{i+ap+b} \subset J_{i+ap}$, we have

$$\big[J_{i+ap+b} + D + (a,0)\big] \cap U \subset \big[J_{i+ap} + D + (a,0)\big] \cap U \subset J_i.$$

Finally, we prove (4.6). We may assume $b \geq 1$, since if $b = 0$, we have

$$\begin{array}{ll} & \big[J_{i+ap} + D + (a+1, -p^2)\big] \cap U \\ \subset & \big[J_{i+ap} + D + (a,0)\big] \cap U \qquad (\text{since } (1,-p^2) \in D) \\ \subset & J_i \qquad (\text{by (4.32)}). \end{array} \tag{4.33}$$

In (iv), if α_i does not exist or $\alpha_i < b$, then $J_{i+b} = \emptyset$. Hence $J_{i+ap+b} = \emptyset$ and we are done. So assume that $\alpha_i \geq b$. By (iv) and the fact that $J_{i+1}, \ldots, J_n$ is backward consistent, we have

$$\begin{cases} \big[J_{i+\alpha_i} + D + (1, -p^2 + p\alpha_i)\big] \cap U \subset J_i, \\ \big[J_{i+b} + D + (0, -p(\alpha_i - b))\big] \cap U \subset J_{i+\alpha_i}, \\ \big[J_{i+ap+b} + D + (a,0)\big] \cap U \subset J_{i+b}. \end{cases} \tag{4.34}$$

If neither of $J_{i+\alpha_i}$ and J_{i+b} is $\emptyset$ or U, by (4.34) and Lemma 4.4, we have

$$\big[J_{i+ap+b} + D + (a+1, -p^2 + pb)\big] \cap U \subset J_i,$$

which is (4.6). If one of $J_{i+\alpha_i}$ and J_{i+b} is $\emptyset$ or U, then $J_{i+b} = \emptyset$ or $J_{i+b} = U$ or $J_{i+\alpha_i} = U$ since $J_{i+\alpha_i} \neq \emptyset$. Thus $J_{i+ap+b} = \emptyset$ or $J_i = U$ and (4.6) also holds. □

Theorem 4.6. *Let i be an integer with $0 \leq i \leq n$. Let $J_0, \ldots, J_{i-1}$ be a forward consistent sequence of ideals of U and let J_i be an ideal of U. Then J_i is consistent with $J_0, \ldots, J_{i-1}$ if and only if the following conditions are satisfied.*

(i) $J_i \subset J_{i-1}$.
(ii) $J_i \supset \big[J_{i-1} + D - (0,p)\big] \cap U$.
(iii) $\big[J_i + D + (1,0)\big] \cap U \subset J_{i-p}$. *(If $i - p < 0$, this condition is null.)*
(iv) *Let β_i be the largest integer such that $1 \leq \beta_i \leq p-1$, $i - \beta_i \geq 0$ and $J_{i-\beta_i} \neq U$. Then $\big[J_i + D + (1, -p^2 + p\beta_i)\big] \cap U \subset J_{i-\beta_i}$. (If such a β_i does not exist, this condition is null.)*

Proof. By the same reason in the proof of Theorem 4.5, we may assume $n \geq p$.

We show that (4.1) – (4.3) in Lemma 4.1 together are equivalent to conditions (i) – (iv) in Theorem 4.6. Since the proof is essentially the same as the proof of Theorem 4.5, we only show that (i) – (iv) of Theorem 4.6 imply (4.3).

Let a, b be integers such that $a \geq 0$, $0 \leq b \leq p-1$ and $i - ap - b \geq 0$. By an argument similar to (4.33), we may assume $b \geq 1$. In (iv), if β_i does not exist or if

$\beta_i < b$, then $J_{i-b} = U$. Hence $J_{i-ap-b} = U$ and (4.3) is obvious. So we may assume that $\beta_i \geq b$. By (iv) and the fact that $J_0, \dots, J_{i-1}$ is forward consistent, we have

$$\begin{cases} \big[J_i + D + (1, -p^2 + p\beta_i)\big] \cap U \subset J_{i-\beta_i}, \\ \big[J_{i-\beta_i} + D + (0, -p(\beta_i - b))\big] \cap U \subset J_{i-b}, \\ \big[J_{i-b} + D + (a, 0)\big] \cap U \subset J_{i-ap-b}. \end{cases} \tag{4.35}$$

If neither of J_{i-b} and $J_{i-\beta_i}$ is $\emptyset$ or U, (4.3) follows from (4.35) and Lemma 4.4. If one of J_{i-b} and $J_{i-\beta_i}$ is $\emptyset$ or U, then $J_{i-b} = \emptyset$ or $J_{i-b} = U$ or $J_{i-\beta_i} = \emptyset$ since $J_{i-\beta_i} \neq U$. Thus $J_{i-ap-b} = U$ or $J_i = \emptyset$; in either case, (4.3) holds. □

Corollary 4.7. (Backward slicing) *Let i be an integer with $0 \leq i \leq n$. Let $J_{i+1}, \dots, J_n$ be a backward consistent sequence of ideals of U and let J_i be an ideal of U. Put $W_j = \omega(J_j)$, $i \leq j \leq n$. Let*

$$\begin{aligned} X_i = W_{i+1} &\vee \big[\underline{\big(W_{i+p} + (1,0)\big)}_{[0,n+1]\times[0,n]}\ \big|_U\big] \\ &\vee \big[\underline{\big(W_{i+\alpha_i} + (1, -p^2 + p\alpha_i)\big)}_{[0,n+1]\times[-p^2+p\alpha_i,n]}\ \big|_U\big], \end{aligned} \tag{4.36}$$

where α_i is defined in Theorem 4.5 (iv)*, and*

$$Y_i = \overline{(W_{i+1})}_{[0,n]\times[-p,n]}\ \big|_{[0,n]\times[-p,-p+n]} + (0,p). \tag{4.37}$$

Then J_i is consistent with $J_{i+1}, \dots, J_n$ if and only if

$$X_i \leq W_i \leq Y_i. \tag{4.38}$$

Note. In (4.36), if $i + p > n$, the walk after the first $\vee$ is not defined; if α_i does not exist, the walk after the second $\vee$ is not defined. Our convention, here and later, is that any undefined walk in a $\vee$ or $\wedge$ operation is ignored.

Proof. The corollary is a restatement of Theorem 4.5 in terms of boundaries. In fact, conditions (i), (iii) and (iv) of Theorem 4.5 are equivalent to

$$\begin{cases} W_i \geq W_{i+1}, \\ W_i \geq \underline{\big(W_{i+p} + (1,0)\big)}_{[0,n+1]\times[0,n]}|_U, \\ W_i \geq \underline{\big(W_{i+\alpha_i} + (1, -p^2 + p\alpha_i)\big)}_{[0,n+1]\times[-p^2+p\alpha_i,n]}|_U. \end{cases}$$

By Lemma 4.2, condition (ii) of Theorem 4.5 is equivalent to

$$W_i \leq \overline{(W_{i+1})}_{[0,n]\times[-p,n]}\ \big|_{[0,n]\times[-p,-p+n]} + (0,p).$$

□

Corollary 4.8. (Forward slicing) *Let i be an integer with $0 \leq i \leq n$. Let $J_0, \dots, J_{i-1}$ be a forward consistent sequence of ideals of U and let J_i be an ideal of U. Put $W_j = \omega(J_j)$, $0 \leq j \leq i$. Let*

$$X_i' = \underline{\big(W_{i-1} - (0,p)\big)}_{[0,n]\times[-p,n]}\ \big|_U \tag{4.39}$$

and

$$\begin{aligned} Y_i' = W_{i-1} \wedge \big[\overline{(W_{i-p})}_{[0,n+1]\times[0,n]}\ \big|_{[1,n+1]\times[0,n]} - (1,0)\big] \wedge \\ \big[\overline{(W_{i-\beta_i})}_{[0,n+1]\times[-p^2+p\beta_i,n]}\ \big|_{[1,n+1]\times[-p^2+p\beta_i,-p^2+p\beta_i+n]} - (1, -p^2 + p\beta_i)\big], \end{aligned} \tag{4.40}$$

where β_i is defined in Theorem 4.6 (iv). *Then J_i is consistent with $J_0, \ldots, J_{i-1}$ if and only if*

$$X_i' \le W_i \le Y_i'. \tag{4.41}$$

Proof. The corollary is a restatement of Theorem 4.6 in terms of boundaries. By Lemma 4.2, conditions (i), (iii) and (iv) of Theorem 4.6 are equivalent to

$$\begin{cases} W_i \le W_{i-1}, \\ W_i \le \overline{(W_{i-p})}_{[0,n+1]\times[0,n]} \big|_{[1,n+1]\times[0,n]} - (1,0), \\ W_i \le \overline{(W_{i-\beta_i})}_{[0,n+1]\times[-p^2+p\beta_i,n]} \big|_{[1,n+1]\times[-p^2+p\beta_i,-p^2+p\beta_i+n]} - (1,-p^2+p\beta_i). \end{cases}$$

Condition (ii) of Theorem 4.6 is equivalent to

$$W_i \ge \underline{\big(W_{i-1} - (0,p)\big)}_{[0,n]\times[-p,n]} \big|_U .$$

□

Example 4.9. (Backward slicing) Let $p = 3$ and $m = 12$ ($n = \frac{m}{3}(p-1) = 8$). A backward consistent sequence of ideals $J_8, J_7, \ldots, J_0$ is illustrated in Figure 16 through their boundary walks $W_8, W_7, \ldots, W_0$. When choosing walk W_i, we first determine the lower bound X_i and the upper bound Y_i defined in Corollary 4.7. Figure 17 shows how Y_1 is determined and Figure 18 shows the procedure to find X_1. The ideal $I = \bigcup_{j=0}^{8}(J_j \times \{j\})$ of $\mathcal{U}$ is depicted in Figure 19.

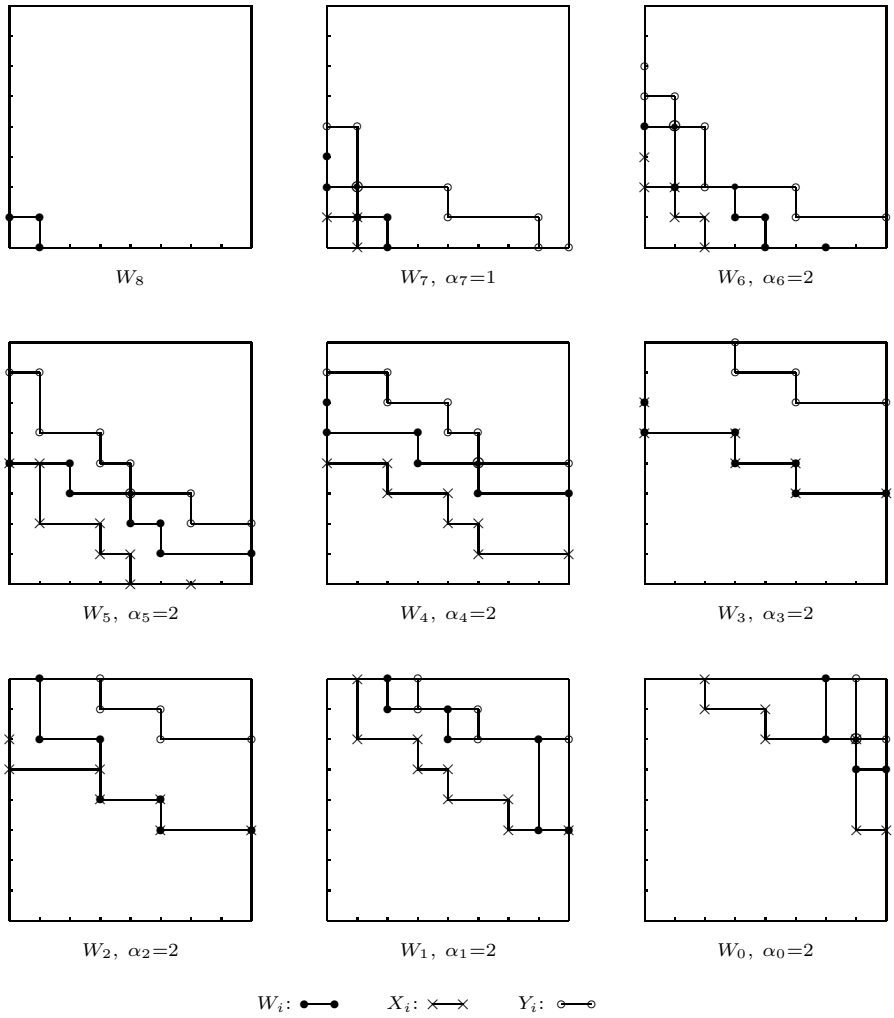

Figure 16. An example of backward slicing

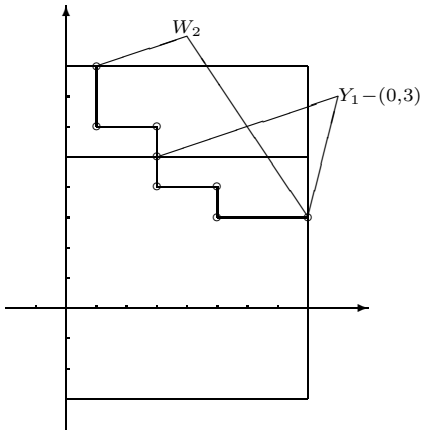

Figure 17. Determination of Y_1

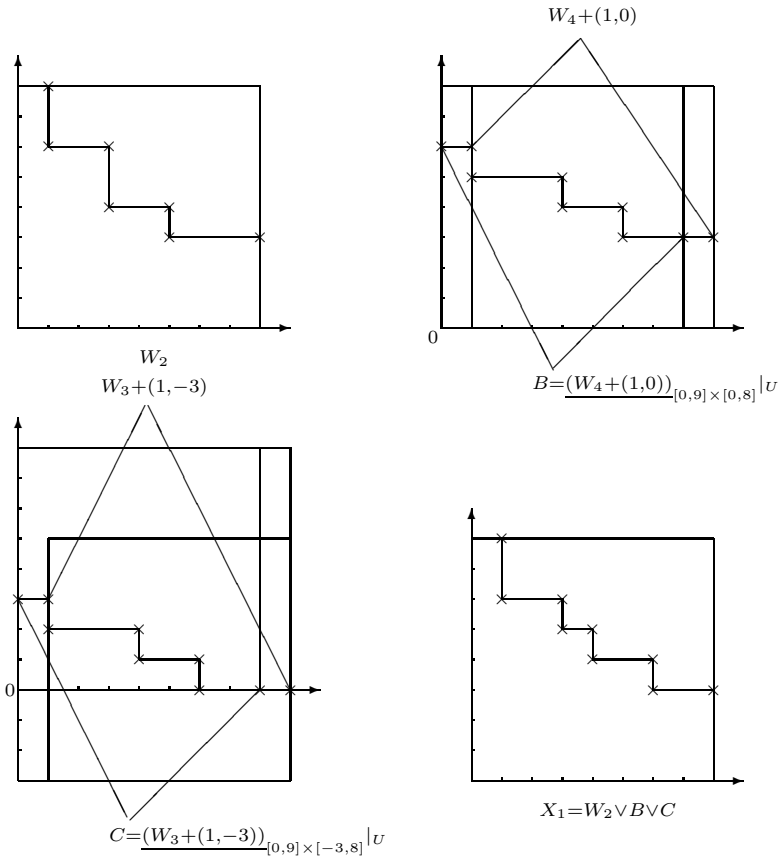

Figure 18. Detremination of X_1

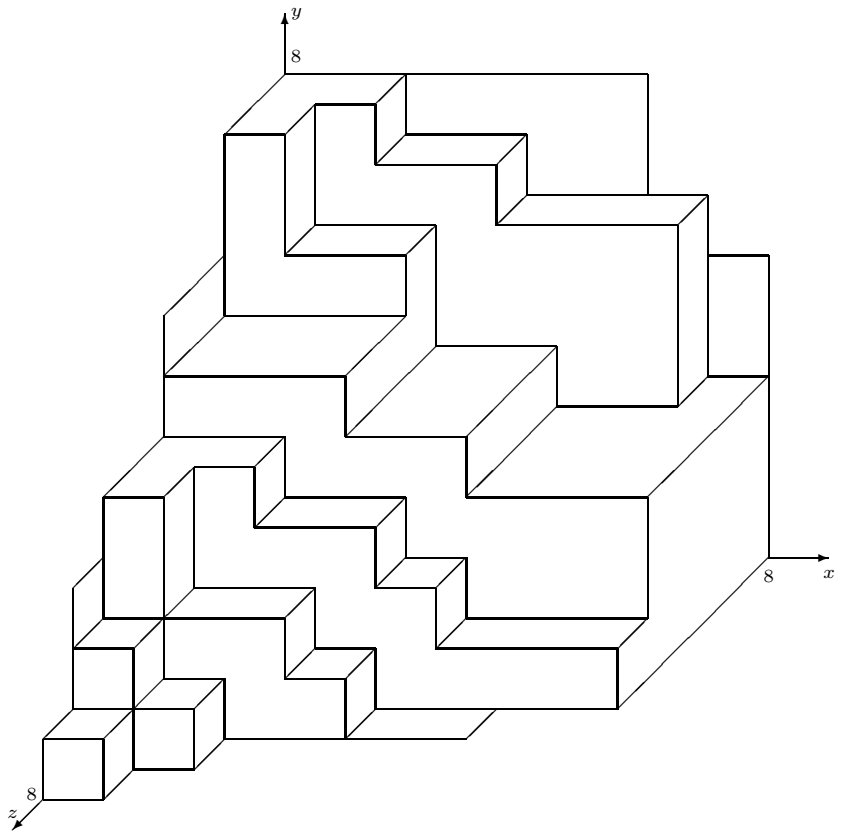

Figure 19. The ideal $I = \bigcup_{j=0}^{8}\big(J_j \times \{j\}\big)$

Example 4.10. (Forward slicing) Let $p = 3$ and $m = 9$ ($n = \frac{m}{3}(p-1) = 6$). A sequence of walks $W_0, W_1, \ldots, W_6$ satisfying (4.41) is given in Figure 20. The resulting ideal $I = \bigcup_{j=0}^{6}(\iota(W_j) \times \{j\})$ of $\mathcal{U}$ is illustrated in Figure 21.

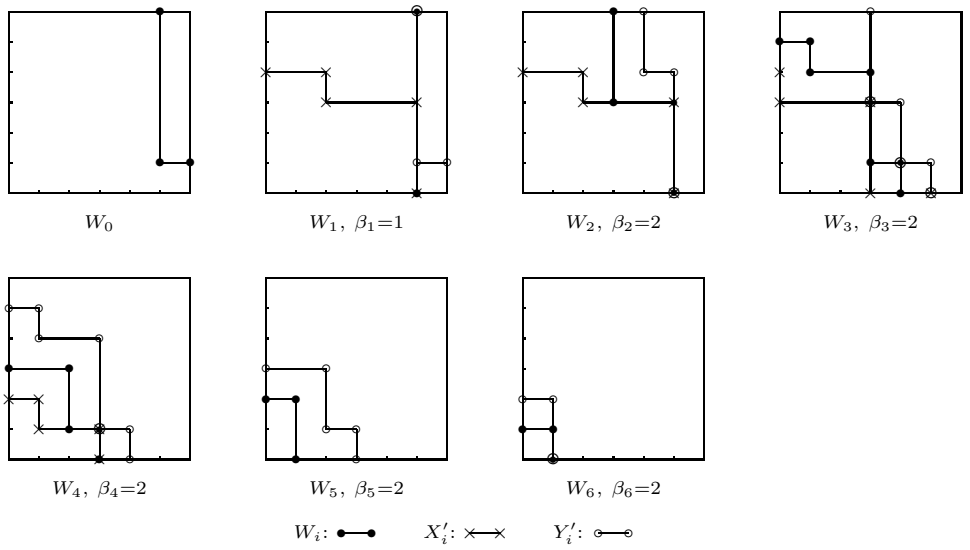

Figure 20. An example of forward slicing

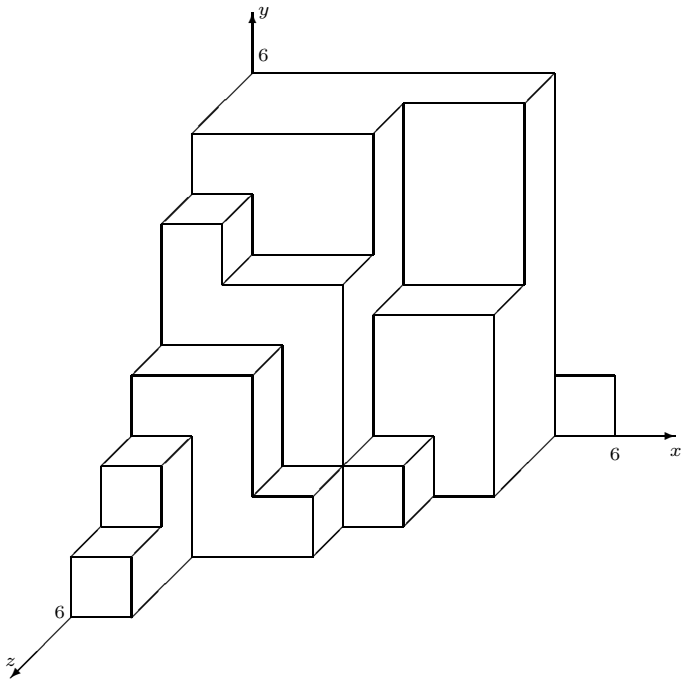

Figure 21. The ideal $I = \bigcup_{j=0}^{6} \big(\iota(W_j) \times \{j\}\big)$

5. Enumerating A-Invariant Ideals of $\mathcal{U}$

In this section, we consider the case $r = 1$. Therefore, we are interested in ideals of $\mathcal{U}$ which are invariant (symmetric) under the action of A. The problem here is more difficult than the one in Section 4.

In order to enumerate the A-invariant ideals of $\mathcal{U}$, we partition $\mathcal{U}$ as

$$\mathcal{U} = \bigcup_{i=0}^{n} \mathcal{V}_i$$

where

$$\mathcal{V}_i = \big\{(x, y, z) \in \mathcal{U} : x \le i,\ y \le i,\ z \le i \text{ and at least one of } x, y, z \text{ is } i\big\}.$$

For any subset $X \subset \mathbb{R}^3$, we denote its image under A, i.e., $\{xA : x \in X\}$, by X^A. Put

$$V_i = [0, i]^2 \times \{i\}.$$

Then

$$\mathcal{V}_i = V_i \cup V_i^A \cup V_i^{A^2}.$$

Let I be an A-invariant ideal of $\mathcal{V}_i$. Write

$$I \cap V_i = J \times \{i\}.$$

Then J is an ideal of $[0, i]^2$ such that

$$I = (J \times \{i\}) \cup (J \times \{i\})^A \cup (J \times \{i\})^{A^2}$$

and

$$\{x : (x, i) \in J\} = \{y : (i, y) \in J\}. \tag{5.1}$$

On the other hand, if J is any subset of $[0, i]^2$ satisfying (5.1), then the A-invariant subset $I = (J \times \{i\}) \cup (J \times \{i\})^A \cup (J \times \{i\})^{A^2} \subset \mathcal{V}_i$ has the property that $I \cap V_i = J \times \{i\}$.

Let J_j $(0 \le j \le i)$ be an ideal of $[0, j]^2$ such that

$$\{x : (x, j) \in J_j\} = \{y : (j, y) \in J_j\}. \tag{5.2}$$

We call the sequence $J_0, \dots, J_{i-1}$ *consistent* if

$$\bigcup_{j=0}^{i-1} \Big[(J_j \times \{j\}) \cup (J_j \times \{j\})^A \cup (J_j \times \{j\})^{A^2}\Big]$$

is an A-invariant ideal of $[0, i-1]^3$. The ideal J_i of $[0, i]^2$ is said to be *consistent* with $J_0, \dots, J_{i-1}$ if the sequence $J_0, \dots, J_{i-1}, J_i$ is consistent. Note that the meaning of consistency here is different from that of Section 4.

Note. In the terminology of Section 2, the statement that J_i is *consistent* with $J_0, \dots, j_{i-1}$ means that $\bigcup_{s=0}^{2} (J_i \times \{i\})^{A^s}$ is *compatible* with $\bigcup_{s=0}^{2} (J_j \times \{j\})^{A^s}$, $0 \le j < i$, with respect to the partition $\mathcal{U} = \bigcup_{j=0}^{n} \mathcal{V}_j$.

Given a consistent sequence of ideals $J_0, \dots, J_{i-1}$ and an ideal J_i of $[0, i]^2$. Our goal in this section, roughly speaking, is to determined two walks Φ_i and Ψ_i in $[0, i]^2$ such that J_i is consistent with $J_0, \dots, J_{i-1}$ if and only if $\Phi_i \le \omega(J_i) \le \Psi_i$.

Lemma 5.1. *Let $0 \le i \le n$. Let J_j $(0 \le j \le i)$ be an ideal of $[0,j]^2$ such that $J_0, \dots, J_{i-1}$ is a consistent sequence. Write*

$$\bigcup_{j=0}^{i-1} \Big[(J_j \times \{j\}) \cup (J_j \times \{j\})^A \cup (J_j \times \{j\})^{A^2} \Big] = \bigcup_{j=0}^{i-1} \big(J_{i,j} \times \{j\} \big), \tag{5.3}$$

where $J_{i,j}$ $(0 \le j \le i-1)$ is a ideal of $[0, i-1]^2$, and write

$$\omega(J_i) = \big((x_0, y_0), \dots, (x_k, y_k) \big).$$

Then J_i is consistent with $J_0, \dots, J_{i-1}$ if and only if the following conditions are satisfied:

$$(x_0, y_0) = (y_k, x_k) \quad \text{if } y_0 = i. \tag{5.4}$$

$$\big(J_i \times \{i\} + \Delta \big) \cap \big([0, i-1]^2 \times \{j\} \big) \subset J_{i,j} \times \{j\} \quad \text{for all } 0 \le j < i. \tag{5.5}$$

$$\big(J_{i,j} \times \{j\} + \Delta \big) \cap V_i \subset J_i \times \{i\} \quad \text{for all } 0 \le j < i. \tag{5.6}$$

$$\big(J_i \times \{i\} + \Delta \big) \cap V_i^A \subset \big(J_i \times \{i\} \big)^A. \tag{5.7}$$

$$\big(J_i \times \{i\} + \Delta \big) \cap V_i^{A^2} \subset \big(J_i \times \{i\} \big)^{A^2}. \tag{5.8}$$

Proof. Let $I = (J_i \times \{i\}) \cup (J_i \times \{i\})^A \cup (J_i \times \{i\})^{A^2}$ and denote by I' the ideal of $[0, i-1]^3$ in (5.3).

($\Rightarrow$) Equation (5.4) follows from (5.2). Since $J_0, \dots, J_{i-1}, J_i$ is a consistent sequence of ideals, $I \cup I'$ is an ideal of $[0,i]^3$. By Lemma 2.1 (ii), we have

$$\begin{cases} (I \cap V_i + \Delta) \cap [0, i-1]^3 \subset I', \\ (I' + \Delta) \cap V_i \subset I \cap V_i, \\ (I \cap V_i + \Delta) \cap V_i^A \subset I \cap V_i^A, \\ (I \cap V_i + \Delta) \cap V_i^{A^2} \subset I \cap V_i^{A^2}. \end{cases}$$

These inclusions are equivalent to (5.5) – (5.8) respectively.

($\Leftarrow$) First, from (5.4), we have

$$\{x : (x,i) \in J_i\} = \{y : (i,y) \in J_i\}.$$

Thus (cf. the statement after (5.1)),

$$I \cap V_i = J_i \times \{i\}. \tag{5.9}$$

From (5.9), (5.7), and (5.8), we have

$$(I \cap V_i + \Delta) \cap V_i^{A^k} \subset I \cap V_i^{A^k}, \quad k = 0, 1, 2.$$

Hence

$$(I \cap V_i + \Delta) \cap \mathcal{V}_i \subset I.$$

Since I is A-invariant, we have

$$(I + \Delta) \cap \mathcal{V}_i \subset I,$$

which means that I is an ideal of $\mathcal{V}_i$.

From (5.9), (5.5), and (5.6), we have

$$\begin{cases}(I\cap V_i+\Delta)\cap[0,i-1]^3\subset I',\\ (I'+\Delta)\cap V_i\subset I\cap V_i.\end{cases}$$

Since both I and I' are A-invariant, we obtain

$$\begin{cases}(I\cap {V_i}^{A^k}+\Delta)\cap[0,i-1]^3\subset I',\\ (I'+\Delta)\cap {V_i}^{A^k}\subset I\cap {V_i}^{A^k},\end{cases}\qquad k=0,1,2.$$

Therefore,

$$\begin{cases}(I+\Delta)\cap[0,i-1]^3\subset I',\\ (I'+\Delta)\cap\mathcal{V}_i\subset I.\end{cases}\tag{5.10}$$

By (5.10) and Lemma 2.1 (ii), $I\cup I'$ is an ideal of $[0,i]^3$, i.e., $J_0,\dots,J_{i-1},J_i$ is consistent. □

Lemma 5.2. *In Lemma 5.1,* (5.4) – (5.6) *imply* (5.7).

Proof. First assume $i<p$. In this case, the partial order $\prec$ in $[0,i]^3$ is the cartesian product of linear orders and (5.7) follows from (5.4) trivially. (See Figure 22.)

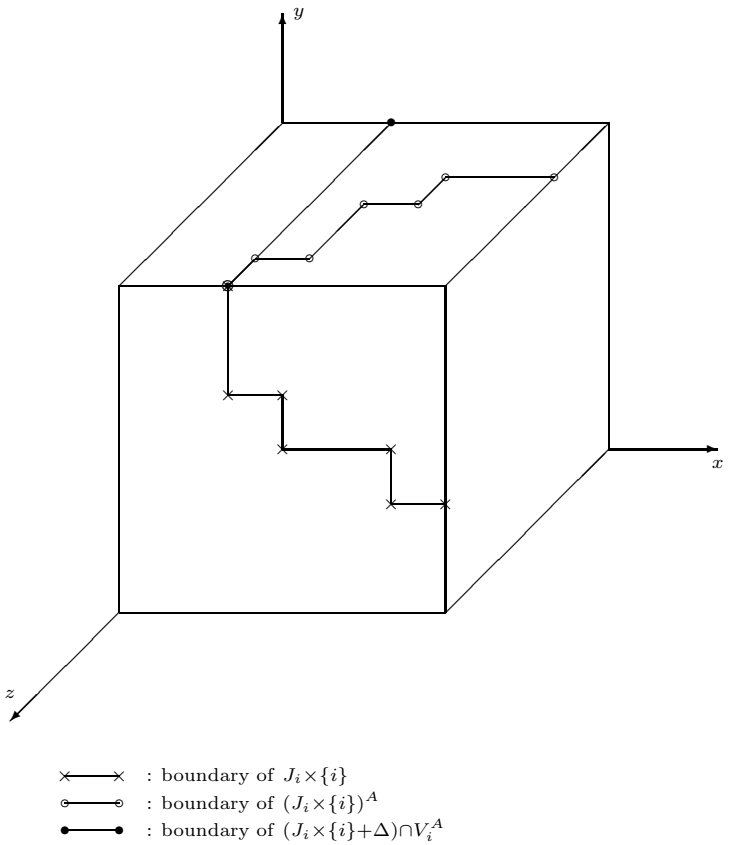

Figure 22. $(J_i\times\{i\}+\Delta)\cap {V_i}^A\subset(J_i\times\{i\})^A$ when $i<p$

So we assume that $i \geq p$. Let I and I' be as in the proof of Lemma 5.1. Note that $I \cap V_i = J_i \times \{i\}$ by (5.4).

For each $u = (x', i, z') \in \big(J_i \times \{i\} + \Delta\big) \cap V_i^A$, we want to show that $u \in (J_i \times \{i\})^A$. Note that there exists $(x, y) \in J_i$ such that $u \prec (x, y, i)$.

If $y = i$, then $(x, y, i) \in (J_i \times \{i\}) \cap V_i^A = I \cap V_i \cap V_i^A \subset (I \cap V_i)^A = (J_i \times \{i\})^A$. Since $(J_i \times \{i\})^A$ is an ideal of V_i^A, we have $u \in (J_i \times \{i\})^A$. Thus we assume $y < i$.

If $z' = i$, then $(x', i, i) \prec (x, y, i)$ implies $(x', i) \prec (x, y)$, hence $(x', i) \in J_i$. By (5.4), $(i, x') \in J_i$, hence $u = (x', i, i) = (i, x', i)A \in (J_i \times \{i\})^A$. Thus we assume $z' < i$.

By (3.6), $(x', i, z') \prec (x, y, i)$ if and only if

$$(x', i, z') \prec (x, i, i) - (i - y)(p, 0, 0) = (x - (i - y)p, i, i).$$

Thus we have

$$\begin{aligned}(x', i, z') &\prec (x', i, z') + (p, -1, 0)\\ &\prec (x - (i - y)p, i, i) + (p, -1, 0)\\ &= (x - (i - 1 - y)p, i - 1, i)\\ &= (x, y, i) + (i - 1 - y)(-p, 1, 0)\\ &\prec (x, y, i),\end{aligned}$$

i.e.,

$$(x', i, z') \prec (x' + p, i - 1, z') \prec (x, y, i). \tag{5.11}$$

If $(z', x') \prec (x, y)$, then $(z', x') \in J_i$. Thus $(x', i, z') = (z', x', i)A \in (J_i \times \{i\})^A$. Therefore, we assume $(z', x') \not\prec (x, y)$.

We claim that

$$x' < i - p. \tag{5.12}$$

In fact, since $(x', i, z') \prec (x - (i - y)p, i, i)$, we have $(z', x') \prec (i, x - (i - y)p)$, i.e.,

$$x' \leq x - (i - y)p + \frac{1}{p}(i - z'). \tag{5.13}$$

If $z' > x$, (5.13) gives

$$\begin{aligned}x' &< x - (i - y)p + \frac{1}{p}(i - x)\\ &= \frac{p - 1}{p}x + py - \frac{p^2 - 1}{p}i\\ &\leq \frac{p - 1}{p}i + p(i - 1) - \frac{p^2 - 1}{p}i\\ &= i - p.\end{aligned}$$

If $z' \leq x$, since $(z', x') \not\prec (x, y)$, we must have

$$x' > y + \frac{1}{p}(x - z'). \tag{5.14}$$

Combining (5.13) and (5.14), we have

$$x - (i - y)p + \frac{1}{p}(i - z') > y + \frac{1}{p}(x - z')$$

which gives

$$(p-1)y > \frac{1}{p}x - x + pi - \frac{1}{p}i = \frac{p^2-1}{p}i - \frac{p-1}{p}x,$$

i.e.,

$$y > \frac{p+1}{p}i - \frac{1}{p}x \geq i,$$

which is a contradiction. Thus (5.12) is proved.

Now we have $(x'+p, i-1, z') \prec (x, y, i)$ and $(x'+p, i-1, z') \in [0, i-1]^3$. By (5.5), $(x'+p, i-1, z') \in (J_i \times \{i\} + \Delta) \cap [0, i-1]^3 \subset I'$. Thus we have

$$\begin{aligned} (x', i, z') &\in (I' + \Delta) \cap V_i^A && \text{(by (5.11))} \\ &\subset (J_i \times \{i\})^A && \text{(by (5.6) and the } A\text{-symmetry of } I'). \end{aligned}$$

□

Lemma 5.3. *Assume that in Lemma 5.1,* (5.4) – (5.7) *are satisfied. Then* (5.8) *is equivalent to*

$$\max\{y : (i-1, y) \in J_i\} \leq \max\{x : (x, i-p) \in J_i\} \quad \text{if } i \geq p. \tag{5.15}$$

Proof. First assume $i < p$. Then (5.15) is satisfied without instance. Since in case, the partial order $\prec$ in $[0, i]^3$ is the cartesian product of linear orders, (5.8) holds trivially. (See Figure 23.) So we assume that $i \geq p$. Again, let I and I' be as in the proof of Lemma 5.1.

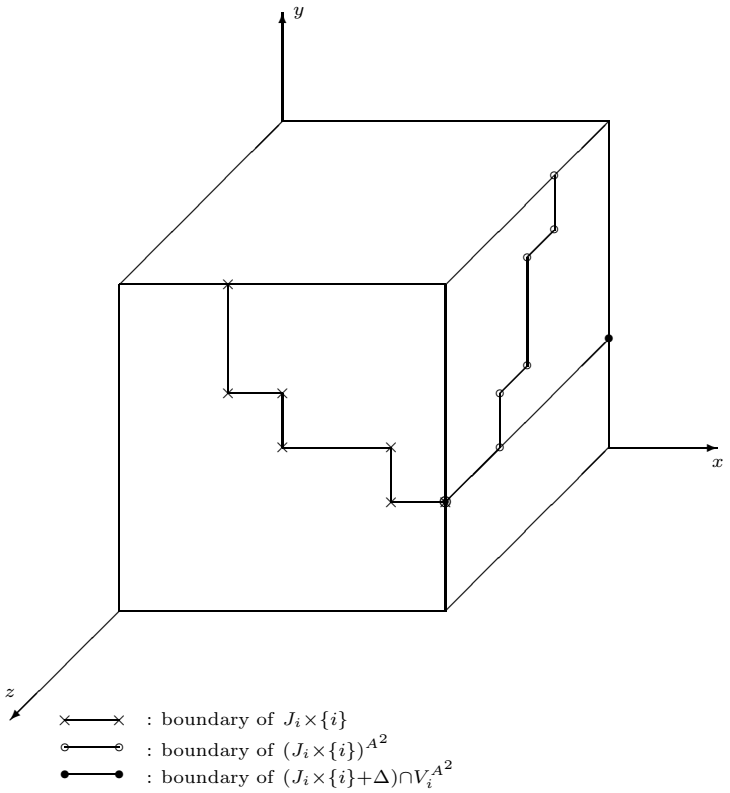

Figure 23. $(J_i \times \{i\} + \Delta) \cap V_i^{A^2} \subset (J_i \times \{i\})^{A^2}$ when $i < p$

Proof of "(5.15) $\Rightarrow$ (5.8)". Let $u = (i, y', z') \in (J_i \times \{i\} + \Delta) \cap V_i^{A^2}$. We want to show that $u \in (J_i \times \{i\})^{A^2}$.

Note that there exists $(x, y) \in J_i$ such that $u \prec (x, y, i)$. Also note that (5.4) implies that $I \cap V_i = J_i \times \{i\}$.

If $x = i$, then $(x, y, i) \in (J_i \times \{i\}) \cap V_i^{A^2} = I \cap V_i \cap V_i^{A^2} \subset (I \cap V_i)^{A^2} = (J_i \times \{i\})^{A^2}$. Since $(J_i \times \{i\})^{A^2}$ is an ideal of $V_i^{A^2}$, we have $u \in (J_i \times \{i\})^{A^2}$.

Next, assume $x < i - 1$. By (3.5), $(i, y', z') \prec (x, y, i)$ if and only if

$$(i, y', z') \prec (i, y, i) - (i - x)(0, 0, p) = (i, y, i - p(i - x)).$$

Thus we have

$$\begin{aligned}(i, y', z') &\prec (i, y, i - p(i - x)) \\ &\prec (i, y, i - p(i - x)) + (i - x - 1)(-1, 0, p) \\ &= (x + 1, y, i - p) \\ &\prec (x, y, i),\end{aligned}$$

i.e.,

$$u = (i, y', z') \prec (x + 1, y, i - p) \prec (x, y, i). \tag{5.16}$$

If $y = i$, then

$$\begin{aligned}(x + 1, y, i - p) &\in (J_i \times \{i\} + \Delta) \cap V_i^A \\ &\subset (J_i \times \{i\})^A \qquad \text{(by (5.7))}.\end{aligned}$$

Thus

$$\begin{aligned}u &\in \big[(J_i \times \{i\})^A + \Delta\big] \cap V_i^{A^2} \\ &\in \big[(J_i \times \{i\} + \Delta) \cap V_i^A\big]^A \\ &\subset (J_i \times \{i\})^{A^2} \qquad \text{(by (5.7) again)}.\end{aligned}$$

If $y < i$, then $(x + 1, y, i - p) \in (J_i \times \{i\} + \Delta) \cap [0, i - 1]^3 \subset I'$. Hence we have

$$\begin{aligned}u &\in (I' + \Delta) \cap V_i^{A^2} \qquad \text{(by (5.16))} \\ &\subset (J_i \times \{i\})^{A^2} \qquad \text{(by (5.6) and the } A\text{-symmetry of } I').\end{aligned}$$

Finally, assume $x = i - 1$. By (3.5), we have

$$\big((x, y, i) + \Delta\big) \cap V_i^{A^2} = \{i\} \times \big[\big((y, i - p) + D\big) \cap [0, i]^2\big].$$

(See Figure 24.) However, by (5.15), $y \le \max\{x : (x, i - p) \in J_i\}$. Thus $(y, i - p) \in J_i$. Therefore,

$$\begin{aligned}u &\in \big((x, y, i) + \Delta\big) \cap V_i^{A^2} \\ &= \{i\} \times \big[\big((y, i - p) + D\big) \cap [0, i]^2\big] \\ &\subset \{i\} \times J_i \\ &= (J_i \times \{i\})^{A^2}.\end{aligned}$$

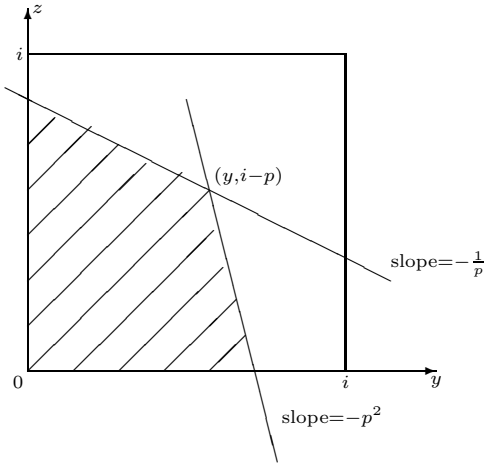

Figure 24. The cross section of $(i-1,y,i)+\Delta$ in $V_i^{A^2}$

Proof of "(5.8) $\Rightarrow$ (5.15)". We may assume that $\{y:(i-1,y)\in J_i\}\neq\emptyset$. Let $\bar{y}=\max\{y:(i-1,y)\in J_i\}$. Then $(i-1,\bar{y})\in J_i$. Hence

$$\begin{aligned}
&\{i\}\times\big[\big((\bar{y},i-p)+D\big)\cap[0,i]^2\big]\\
=\ &\big((i-1,\bar{y},i)+\Delta\big)\cap V_i^{A^2} && \text{(by (3.5))}\\
\subset\ &(J_i\times\{i\}+\Delta)\cap V_i^{A^2}\\
\subset\ &(J_i\times\{i\})^{A^2} && \text{(by (5.8))}\\
=\ &\{i\}\times J_i.
\end{aligned}$$

In particular, $(\bar{y},i-p)\in J_i$. Therefore

$$\bar{y}\le\max\{x:(x,i-p)\in J_i\},$$

which is (5.15). □

Lemma 5.4. *Let J be an ideal of $[0,i-1]^2$ and K an ideal of $[0,i]^2$. Let $b\ge 0$ be an integer. Then*

$$[J+D+(0,-b)]\cap[0,i]^2\subset K \tag{5.17}$$

if and only if

$$[J+D+(0,-b)]\cap[0,i-1]^2\subset K\cap[0,i-1]^2. \tag{5.18}$$

Proof. We only have to prove that (5.18) $\Rightarrow$ (5.17). Let $(x,y)\in[J+D+(0,-b)]\cap[0,i]^2$, we want to show that $(x,y)\in K$.

If $(x,y)\in[0,i-1]^2$, we are done by (5.18). So assume $(x,y)\notin[0,i-1]^2$, i.e., $x=i$ or $y=i$.

There exists $(x',y')\in J+(0,-b)$ such that $(x,y)\prec(x',y')$. If $y'\ge 0$, then $(x',y')\in[0,i-1]^2$, hence $(x',y')\in[J+D+(0,-b)]\cap[0,i-1]^2\subset K\cap[0,i-1]^2\subset K$. Therefore $(x,y)\in K$.

If $y'<0$, since $(x,y)\prec(x',y')$, we must have $x<x'$. By the assumption, $y=i$. From Figure 25, we have

$$(x,i)\prec\big(x'-(i-1-y')p,\ i-1\big)\prec(x',y')$$

and

$$x' - (i-1-y')p \in [x, x'] \subset [0, i-1].$$

Hence $\big(x' - (i-1-y')p,\, i-1\big) \in [J + D + (0,-b)] \cap [0,i-1]^2 \subset K \cap [0,i-1]^2 \subset K$. Therefore, we also have $(x,y) \in K$. □

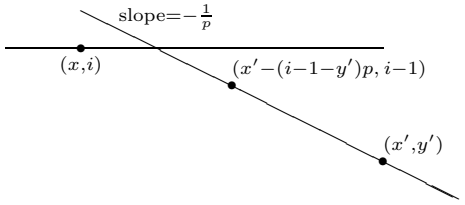

Figure 25. Proof of Lemma 5.4

Lemma 5.5. *Let J and K be ideals of $[0,i-1]^2$ where $i \geq p$ and $J \neq [0,i-1]^2$, $J \neq \emptyset$. Let $b, c \geq 0$ be integers. Let $\hat{J}$ be the largest ideal of $[0,i]^2$ such that $\hat{J} \cap [0,i-1]^2 = J$ and $\hat{K}$ the largest ideal of $[0,i]^2$ such that $\hat{K} \cap [0,i-1]^2 = K$. If*

$$\big[J + (b,-c) + D\big] \cap [0,i-1]^2 \subset K, \tag{5.19}$$

then

$$\big[\hat{J} + (b,-c) + D\big] \cap [0,i]^2 \subset \hat{K}. \tag{5.20}$$

Proof. Let $\omega(J) = W$ and $\omega(K) = Z$. Then $\omega(\hat{K}) = \overline{Z}_{[0,i]^2}$,

$$\omega\big(\hat{J} + (b,-c)\big) = \overline{(W + (b,-c))}_{[b,b+i]\times[-c,-c+i]},$$

and

$$\begin{aligned} \omega\big(\big[\hat{J} + (b,-c) + D\big] \cap [0,i]^2\big) &= \underline{\omega(\hat{J} + (b,-c))}_{[0,b+i]\times[-c,i]} \,\big|_{[0,i]^2} \\ &= Y|_{[0,i]^2}, \end{aligned} \tag{5.21}$$

where

$$Y = \underline{\big[\overline{(W + (b,-c))}_{[b,b+i]\times[-c,-c+i]}\big]}_{[0,b+i]\times[-c,i]}.$$

Since $J \neq [0,i-1]^2$ and $J \neq \emptyset$, we have $\hat{J} \neq [0,i]^2$ and $\hat{J} \neq \emptyset$. Thus $\omega(\hat{J}+(b,-c))$ is neither $\emptyset$ nor the single point $(b+i,-c+i)$. Since $i \geq p$, $\omega(\hat{J}+(b,-c))$ is not a single horizontal step. Therefore, the extension from $\omega(\hat{J}+(b,-c))$ to Y requires the same additional steps as the extension from $W + (b,-c)$ to $\underline{(W + (b,-c))}_{[0,b+i-1]\times[-c,i]}$. (See Figure 26.) Thus Y is the union (in the obvious sense) of

$$\underline{(W + (b,-c))}_{[0,b+i-1]\times[-c,i]} \quad \text{and} \quad \omega(\hat{J} + (b,-c)). \tag{5.22}$$

By (5.19), we have

$$\underline{(W + (b,-c))}_{[0,b+i-1]\times[-c,i-1]} \,\big|_{[0,i-1]^2} \leq Z. \tag{5.23}$$

By (5.22), Y is an extension of $\underline{(W + (b,-c))}_{[0,b+i-1]\times[-c,i]}$, hence an extension of $\underline{(W + (b,-c))}_{[0,b+i-1]\times[-c,i-1]} \,\big|_{[0,i-1]^2}$. Thus (5.23) gives $Y \leq \overline{Z}_{[0,b+i,]\times[-c,i]}$. Taking restriction on $[0,i]^2$, we have

$$Y|_{[0,i]^2} \leq \overline{Z}_{[0,i]^2}.$$

Using (5.21), we have

$$\omega\Big(\big[\hat{J}+(b,-c)+D\big]\cap[0,i]^2\Big)\le \overline{Z}_{[0,i]^2}=\omega(\hat{K}),$$

which proves (5.20). □

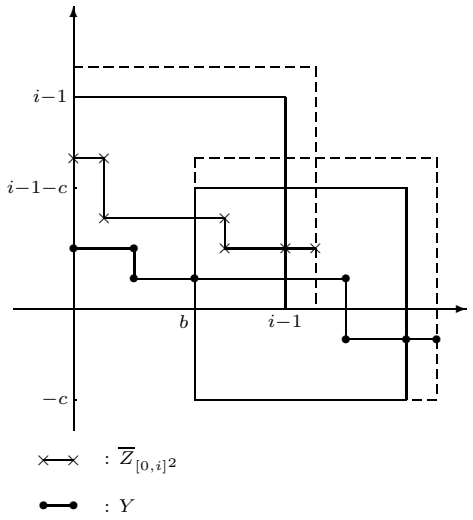

Figure 26. Proof of Lemma 5.5

Lemma 5.6. *In Lemma 5.1, let $W_{i,j}=\omega(J_{i,j})$ $(0\le j<i)$ and $W_i=\omega(J_i)$. Set*

$$S_i=\underline{(W_{i,i-1}+(0,-p))}_{[0,i]\times[-p,i]}\,\big|_{[0,i]^2} \tag{5.24}$$

and

$$\begin{aligned}T_i=&\overline{(W_{i,i-1})}_{[0,i]^2}\wedge\big[\overline{(W_{i,i-p})}_{[0,1+i]\times[0,i]}\,\big|_{[1,1+i]\times[0,i]}-(1,0)\big]\wedge\\&\big[\overline{(W_{i,i-\beta_i})}_{[0,1+i]\times[-p^2+p\beta_i,i]}\,\big|_{[1,1+i]\times[-p^2+p\beta_i,-p^2+p\beta_i+i]}-(1,-p^2+p\beta_i)\big],\end{aligned} \tag{5.25}$$

where β_i is the largest integer such that $1\le\beta\le p-1$, $i-\beta_i\ge 0$ and $J_{i,i-\beta_i}\ne[0,i-1]^2$. (If β_i does not exist, the last walk at the right hand side of (5.25) is ignored.) Then (5.5) *and* (5.6) *hold if and only if*

$$S_i\le W_i\le T_i.$$

Proof. We will show that (5.6) is equivalent to $S_i\le W_i$ and that (5.5) is equivalent to $W_i\le T_i$.

First we claim that (5.6) is equivalent to

$$\big[J_{i,j}+D-(i-j)(0,p)\big]\cap[0,i]^2\subset J_i\quad\text{for all } 0\le j<i \tag{5.26}$$

and that (5.5) is equivalent to

$$\big[J_i+D+(a,0)\big]\cap[0,i-1]^2\subset J_{i,i-ap-b} \tag{5.27}$$

and

$$\big[J_i+D+(a+1,-p^2+bp)\big]\cap[0,i-1]^2\subset J_{i,i-ap-b}, \tag{5.28}$$

where $a, b \in \mathbb{Z},\ a \geq 0,\ 0 \leq b \leq p-1$ and $ap+b \leq i$. The proof of these claims is the same as the proof of Lemma 4.1 (i).

Therefore, it suffices to establish the following relations:

(5.26) $\Leftrightarrow S_i \leq W_i$;
(5.27) and (5.28) $\Leftrightarrow W_i \leq T_i$.

Proof of "(5.26) $\Leftrightarrow S_i \leq W_i$". By Lemma 5.4, (5.26) is equivalent to

$$\big[J_{i,j} + D - (i-j)(0,p)\big] \cap [0,i-1]^2 \subset J_i \cap [0,i-1]^2 \quad \text{for all } 0 \leq j < i. \tag{5.29}$$

Since $\bigcup_{j=0}^{i-1}(J_{i,j} \times \{j\})$ is an ideal of $[0,i-1]^3$, we have (cf. (4.1))

$$\big[J_{i,j} + D - (i-1-j)(0,p)\big] \cap [0,i-1]^2 \subset J_{i,i-1} \quad \text{for all } 0 \leq j < i. \tag{5.30}$$

Note that Lemma 4.3 remains true with $[0,i-1]^2$ in place of U. Thus by Lemma 4.3 and (5.30), we see that (5.29) holds for all $0 \leq j < i$ if and only if it holds for $j = i-1$, i.e., if and only if

$$\big[J_{i,i-1} + D - (0,p)\big] \cap [0,i-1]^2 \subset J_i \cap [0,i-1]^2. \tag{5.31}$$

By Lemma 5.4 again, (5.31) is equivalent to

$$\big[J_{i,i-1} + D - (0,p)\big] \cap [0,i]^2 \subset J_i. \tag{5.32}$$

In terms of boundaries, (5.32) is equivalent to $S_i \leq W_i$.

Proof of "(5.27) and (5.28) $\Leftrightarrow W_i \leq T_i$". Let $\hat{J}_{i,j}$ $(0 \leq j < i)$ be the largest ideal of $[0,i]^2$ such that $\hat{J}_{i,j} \cap [0,i-1]^2 = J_{i,j}$. We claim that $W_i \leq T_i$ is equivalent to the following three conditions:

$$J_i \subset \hat{J}_{i,i-1}. \tag{5.33}$$

$$\big[J_i + D + (1,0)\big] \cap [0,i]^2 \subset \hat{J}_{i,i-p} \quad \text{if } i \geq p. \tag{5.34}$$

$$\big[J_i + D + (1,-p^2+p\beta_i)\big] \cap [0,i]^2 \subset \hat{J}_{i,i-\beta_i}. \tag{5.35}$$

(If β_i does not exist, condition (5.35) is null.)

In fact, (5.33) is equivalent to

$$W_i \leq \overline{(W_{i,i-1})}_{[0,i]^2}.$$

By Lemma 4.2, (5.34) is equivalent to

$$\begin{aligned} W_i + (1,0) &\leq \overline{\big(\overline{(W_{i,i-p})}_{[0,i]^2}\big)}_{[0,1+i]\times[0,i]} \big|_{[1,1+i]\times[0,i]} \\ &= \overline{(W_{i,i-p})}_{[0,1+i]\times[0,i]} \big|_{[1,1+i]\times[0,i]}, \end{aligned}$$

and (5.35) is equivalent to

$$\begin{aligned} &W_i + (1,-p^2+p\beta_i) \\ &\leq \overline{\big(\overline{(W_{i,i-\beta_i})}_{[0,i]^2}\big)}_{[0,1+i]\times[-p^2+p\beta_i,i]} \big|_{[1,1+i]\times[-p^2+p\beta_i,-p^2+p\beta_i+i]} \\ &= \overline{(W_{i,i-\beta_i})}_{[0,1+i]\times[-p^2+p\beta_i,i]} \big|_{[1,1+i]\times[-p^2+p\beta_i,-p^2+p\beta_i+i]}. \end{aligned}$$

Thus (5.33) – (5.35) together are equivalent to $W_i \leq T_i$.

Therefore, it remains to show that (5.27) and (5.28) $\Leftrightarrow$ (5.33) – (5.35).

Proof of "(5.27) and (5.28) $\Rightarrow$ (5.33) – (5.35)". In (5.27), letting $a = 0$ and $b = 1$, we obtain

$$J_i \cap [0, i-1]^2 \subset J_{i,i-1}.$$

Hence $J_i \subset \hat{J}_{i,i-1}$. In a similar way, (5.34) follows from (5.27) with $a = 1$, $b = 0$; (5.35) follows from (5.28) with $a = 0$, $b = \beta_i$.

Proof of "(5.27) and (5.28) $\Leftarrow$ (5.33) – (5.35)". First assume $i < p$. In this case, the partial order $\prec$ in $[0, i]^3$ is the cartesian product of linear orders. Recall that (5.27) and (5.28) together are equivalent to (5.5) and note that (5.5) is equivalent to

$$(J_i \times \{i\} + \Delta) \cap [0, i-1]^3 \subset \bigcup_{j=0}^{i-1} (J_{i,j} \times \{j\}).$$

Thus it suffices to show that

$$J_i \cap [0, i-1]^2 \subset J_{i,j} \quad \text{for all } 0 \le j < i. \tag{5.36}$$

Since $\bigcup_{j=0}^{i-1}(J_{i,j} \times \{j\})$ is an ideal of $[0, i-1]^3$, we have $J_{i,j} \subset J_{i,j-1}$ for all $0 \le j < i$. By (5.33), we also have $J_i \cap [0, i-1]^2 \subset J_{i,i-1}$. Hence (5.36) holds.

Now assume $i \ge p$. Since $\bigcup_{j=0}^{i-1}(J_{i,j} \times \{j\})$ is an ideal of $[0, i-1]^3$, by Lemma 4.1 (i), we have

$$\begin{cases} [J_{i,j} + D + (a, 0)] \cap [0, i-1]^2 \subset J_{i,j-ap-b} \\ [J_{i,j} + D + (a+1, -p^2 + bp)] \cap [0, i-1]^2 \subset J_{i,j-ap-b} \end{cases}$$

for $a \ge 0,\ 0 \le b \le p-1$ and $ap + b \le j < i$. By Lemma 5.5, we have

$$\begin{cases} [\hat{J}_{i,j} + D + (a, 0)] \cap [0, i]^2 \subset \hat{J}_{i,j-ap-b} \\ [\hat{J}_{i,j} + D + (a+1, -p^2 + bp)] \cap [0, i]^2 \subset \hat{J}_{i,j-ap-b} \end{cases} \tag{5.37}$$

for $a \ge 0,\ 0 \le b \le p-1$ and $ap + b \le j < i$. Note that β_i is also the largest integer such that $1 \le \beta_i \le p-1$, $i - \beta_i \ge 0$ and $\hat{J}_{i,i-\beta_i} \ne [0, i]^2$. By (5.34), (5.35), (5.37) and the proof of Theorem 4.6, we have

$$\begin{cases} [J_i + D + (a, 0)] \cap [0, i]^2 \subset \hat{J}_{i,i-ap-b} \\ [J_i + D + (a+1, -p^2 + bp)] \cap [0, i]^2 \subset \hat{J}_{i,i-ap-b} \end{cases} \tag{5.38}$$

for $a \ge 0,\ 0 \le b \le p-1$ and $ap + b \le j < i$. Conditions (5.27) and (5.28) immediately follow form (5.38). □

Remark. In Lemma 5.6, we always have

$$S_i \le T_i.$$

In fact, by Lemma 2.1 (i), there is at least one J_i satisfying all the conditions in Lemma 5.1. Thus there exists at least one walk W_i in $[0, i]^2$ such that $S_i \le W_i \le T_i$.

Definition 5.7. Let $0 \le i \le n$ and let J_i be an ideal of $[0, i]^2$. We call J_i of

type I if $J_i \cap ([i-1, i] \times [0, i]) = \emptyset$;
type II if $J_i \cap ([i-1, i] \times [0, i]) \ne \emptyset$ but $J_i \cap (\{i\} \times [0, i]) = \emptyset$;
type III if $J_i \cap (\{i\} \times [0, i]) \ne \emptyset$.

Theorem 5.8. *Let $1 \le i \le n$ and let J_j $(0 \le j \le i)$ be an ideal $[0,j]^2$. Assume that $J_0, \dots, J_{i-1}$ is a consistent sequence of ideals and write*

$$\bigcup_{j=0}^{i-1} \big[(J_j \times \{j\}) \cup (J_j \times \{j\})^A \cup (J_j \times \{j\})^{A^2}\big] = \bigcup_{j=0}^{i-1} (J_{i,j} \times \{j\}),$$

where $J_{i,j}$ is an ideal of $[0,i-1]^2$. Let $W_{i,j} = \omega(J_{i,j})$ $(0 \le j < i)$ and $W_i = \omega(J_i)$ and let S_i and T_i be as in Lemma 5.6.

(i) *J_i is of type I and consistent with $J_0, \dots, J_{i-1}$ if and only if*

$$(0,i) \notin \iota(S_i), \quad (i-1,0) \notin \iota(S_i) \tag{5.39}$$

and

$$S_i \le W_i \le T_i',$$

where

$$T_i' = T_i \wedge A_i \wedge B_i,$$

A_i is the highest walk in $[0,i]^2$ starting from $(0,i-1)$ and B_i is the highest walk in $[0,i]^2$ ending at $(i-2,0)$.

(ii) *J_i is of type II and consistent with $J_0, \dots, J_{i-1}$ if and only if*

$$(0,i) \notin \iota(S_i), \quad (i,0) \notin \iota(S_i) \tag{5.40}$$

and

$$\begin{cases} W_i|_{[i-1,i]\times[0,i]} = \big((i-1,v),\ (i-1,0)\big) \\ \Gamma_i \le W_i|_{[0,i-1]\times[0,i]} \le \Lambda_i \end{cases}$$

for some integer v satisfying

$$\begin{cases} 0 \le v < \min\{p^2, \frac{p-1}{p} i + \frac{1}{p}\} \\ (i-1,v) \in \iota(T_i),\ (i-1,v+i) \notin \iota(X_i) \\ (v,i-p) \in \iota(T_i) \quad \text{if } i \ge p \end{cases} \tag{5.41}$$

and for the walks Γ_i and Λ_i defined as follows.

$$\Gamma_i = (S_i \vee E_{i,v})|_{[0,i-1]\times[0,i]} \vee C_{i,v},$$
$$\Lambda_i = (T_i \wedge A_i)|_{[0,i-1]\times[0,i]} \wedge D_{i,v},$$

where $C_{i,v}$ is the lowest walk in $[0,i-1]\times[0,i]$ ending at $(i-1,v)$, $D_{i,v}$ is the highest walk in $[0,i-1]\times[0,i]$ ending at $(i-1,v)$, and

$$E_{i,v} = \begin{cases} \text{the lowest walk in } [0,i]^2 \text{ passing through } (v,i-p), & \text{if } i \ge p, \\ \emptyset, & \text{if } i < p. \end{cases}$$

(iii) *J_i is of type III and consistent with $J_0, \dots, J_{i-1}$ if and only if*

$$\Phi_i \le W_i \le \Psi_i$$

for some integer u satisfying

$$\begin{cases} 0 \le u \le i \\ (i,u) \in \iota(T_i),\ (u,i) \in \iota(T_i) \\ (i,u+1) \notin \iota(S_i),\ (u+1,i) \notin \iota(S_i) \end{cases} \tag{5.42}$$

and for the walks Φ_i and Ψ_i defined as follows.

$$\Phi_i = S_i \vee F_{i,u} \vee M_{i,u},$$
$$\Psi_i = T_i \wedge G_{i,u} \wedge N_{i,u},$$

where $F_{i,u}$ is the lowest walk in $[0,i]^2$ starting from (u,i), $G_{i,u}$ is the highest walk in $[0,i]^2$ starting from (u,i), $M_{i,u}$ is the lowest walk in $[0,i]^2$ ending at (i,u), $N_{i,u}$ is the highest walk in $[0,i]^2$ ending at (i,u).

Proof. Necessity. We first show the necessity in cases (i) – (iii). By Lemma 5.6, we have $S_i \le W_i \le T_i$.

(i) Since J_i is of type I, $(i-1,0) \notin J_i$. By (5.4), $(0,i) \notin J_i$. Thus $(0,i) \notin \iota(S_i)$, $(i-1,0) \notin \iota(S_i)$ and $W_i \le A_i \wedge B_i$. Hence $W_i \le T_i'$.

(ii) Since J_i is of type II, we have

$$W_i|_{[i-1,i]\times[0,i]} = \big((i-1,v),\,(i-1,0)\big)$$

for some $0 \le v \le i$. Since $(i,0) \notin J_i$, by (5.4), $(0,i) \notin J_i$. Thus $(i-1,v) \in J_i$ implies that $v < p^2$ and $v + (i-1)\frac{1}{p} < i$, i.e.,

$$v < \min\big\{p^2,\ \frac{p-1}{p}i + \frac{1}{p}\big\}.$$

Clearly, $(0,i) \notin \iota(S_i)$, $(i,0) \notin \iota(S_i)$, $(i-1,v) \in \iota(T_i)$ and $(i-1,v+1) \notin \iota(S_i)$. By (5.15), $(v,i-p) \in J_i \subset \iota(T_i)$ if $i \ge p$.

Since $W_i|_{[0,i-1]\times[0,i]}$ ends at $(i-1,v)$, we have

$$C_{i,v} \le W_i|_{[0,i-1]\times[0,i]} \le D_{i,v}. \tag{5.43}$$

Since $(0,i) \notin J_i$, we have $W \le A_i$. In case $i \ge p$, Lemma 5.3 implies $(v,i-p) \in J_i$. Thus, whether $i \ge p$ or not, we always have $W \ge E_{i,v}$. It follows that

$$S_i \vee E_{i,v} \le W_i \le T_i \wedge A_i. \tag{5.44}$$

Combining (5.43) and (5.44), we get

$$\Gamma_i \le W_i|_{[0,i-1]\times[0,i]} \le \Lambda_i.$$

(iii) Assume that W_i ends at (i,u). By (5.4), W_i starts with (u,i). Thus $F_{i,u} \le W_i \le G_{i,u}$ and $M_{i,u} \le W_i \le N_{i,u}$. It follows that $\Phi_i \le W_i \le \Psi_i$. Condition (5.42) is obvious.

Sufficiency. For the sufficiency in cases (i) – (iii), we only give the proof for case (iii). The proofs for cases (i) and (ii) are similar.

By Lemmas 5.1 and 5.2, it suffice to show that conditions (5.4) – (5.6) and (5.8) are satisfied. Since

$$F_{i,u} \vee M_{i,u} \le W_i \le G_{i,u} \wedge N_{i,u},$$

W_i must start from (u,i) and end at (i,u). Hence (5.4) holds. Since $S_i \le W_i \le T_i$, by Lemma 5.6, (5.5) and (5.6) follow. Let $v = \max\{y : (i-1,y) \in J_i\}$. Then $v - u \le p^2$. Thus $(v,i-p) \prec (u+p^2,i-p) \prec (u,i) \in J_i$. Hence $(v,i-p) \in J_i$ and consequently, (5.15) holds. By Lemma 5.3, (5.8) follows. □

Lemma 5.9. *In case* (i) *of Theorem 5.8, condition* (5.39) *implies*

$$S_i \le T_i'. \tag{5.45}$$

In case (ii)*, conditions* (5.40) *and* (5.41) *imply*

$$\Gamma_i \le \Lambda_i. \tag{5.46}$$

In case (iii)*, condition* (5.42) *implies*

$$\Phi_i \le \Psi_i. \tag{5.47}$$

Remark. Lemma 5.9 assures the existence of W_i in Theorem 5.8 provided condition (5.39) in case (i), or conditions (5.40) and (5.41) in case (ii), or condition (5.42) in case (iii) are satisfied.

Proof of Lemma 5.9. It is obvious that (5.39) implies (5.45) and that (5.42) implies (5.47). We only prove that (5.40) and (5.41) imply (5.46).

We show that each of the walks $S_i|_{[0,i-1]\times[0,i]}$, $E_{i,v}|_{[0,i-1]\times[0,i]}$ and $C_{i,v}$ is $\le$ each of the walks $T_i|_{[0,i-1]\times[0,i]}$, $A_i|_{[0,i-1]\times[0,i]}$ and $D_{i,v}$. Most of these relations are obvious. The only ones that need proofs are

$$E_{i,v}|_{[0,i-1]\times[0,i]} \le A_i|_{[0,i-1]\times[0,i]}, \tag{5.48}$$

$$E_{i,v}|_{[0,i-1]\times[0,i]} \le D_{i,v}, \tag{5.49}$$

$$C_{i,v} \le A_i|_{[0,i-1]\times[0,i]}. \tag{5.50}$$

To prove (5.48), we may assume $i \ge p$. It suffices to show that $(0,i) \notin \iota(E_{i,v})$, i.e., $i - p + \frac{1}{p}v < i$. (See Figure 27(a).) This is true since $v < p^2$.

To prove (5.49), we may again assume $i \ge p$. It suffices to show that $i - p \le v + (i-1-v)p^2$, i.e., $v \le i - \frac{p}{p+1}$. (See Figure 27(b).) This follows from the inequality $v < \frac{p-1}{p}i + \frac{1}{p}$ in (5.41).

To prove (5.50), it suffices to have $v + \frac{1}{p}(i-1) < i$. (See Figure 27(c).) This is given by (5.41). □

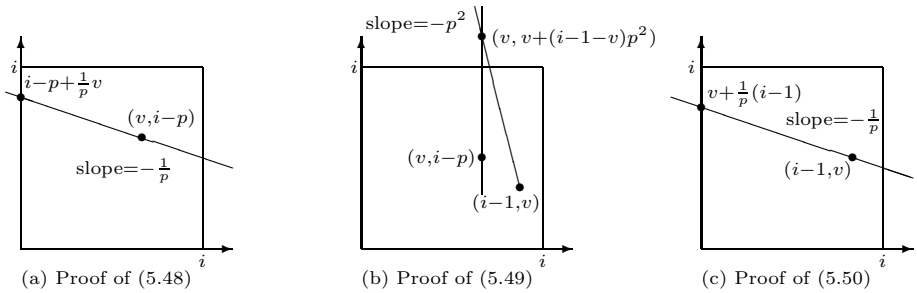

Figure 27. Proofs of (5.48) – (5.50)

Example 5.10. Let $p = 3$ and $m = 9$ ($n = \frac{m}{3}(p-1) = 6$). In this example, we exhibit a consistent sequence of ideals $J_0, \ldots, J_6$ using Theorem 5.8. Figure 28 gives the boundaries $W_i = \omega(J_i)$ $(0 \le i \le 6)$ and the walks S_i and T_i which are needed for choosing W_i. The resulting A-invariant ideal of $[0,6]^3$,

$$I = \bigcup_{i=0}^{6} \Big[(J_i \times \{j\}) \cup (J_i \times \{j\})^A \cup (J_i \times \{j\})^{A^2} \Big],$$

is depicted in Figure 30. The cross sections of I on the parallels of the xy-planes, i.e., $J_{6,0}, \ldots, J_{6,5}, J_6$ are given in Figure 29 in terms of their boundaries $W_{6,0}, \ldots, W_{6,5}, W_6$. The A-symmetry of I is clearly visible in Figure 30. However, the fact that I is an ideal in $(\mathcal{U}, \prec)$ is not obvious from Figure 30.

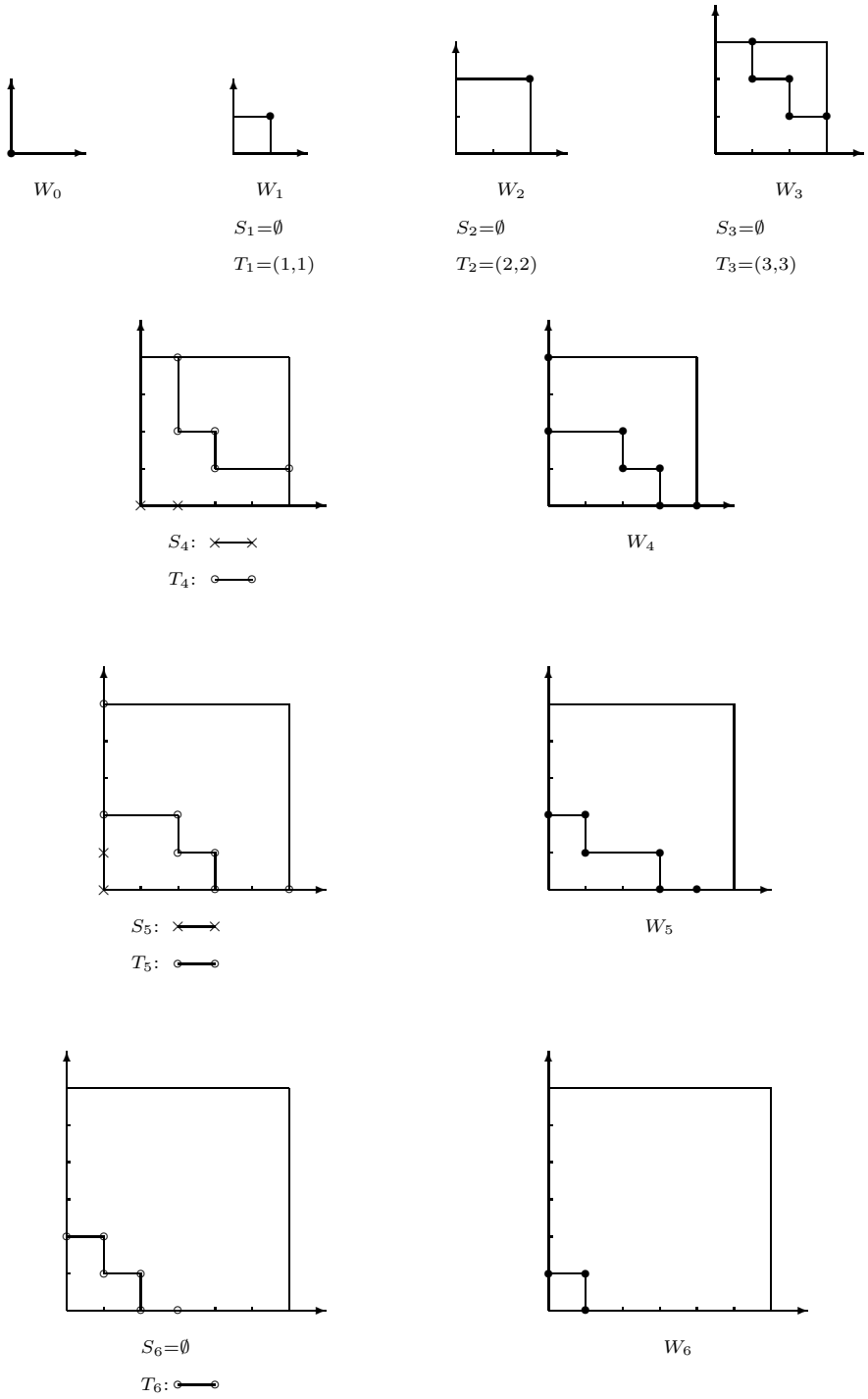

Figure 28. Example 5.10, the walks S_i, T_i and W_i

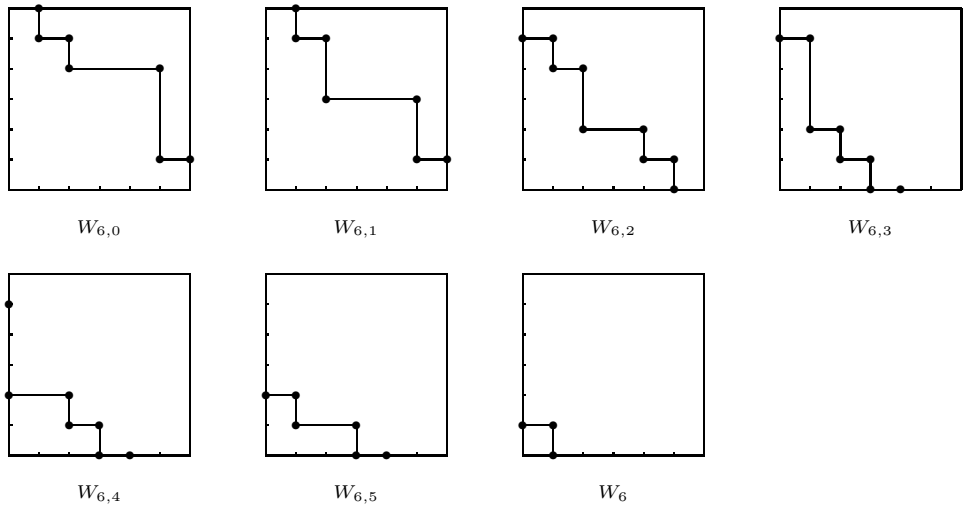

Figure 29. Example 5.10, boundaries of the cross sections of I

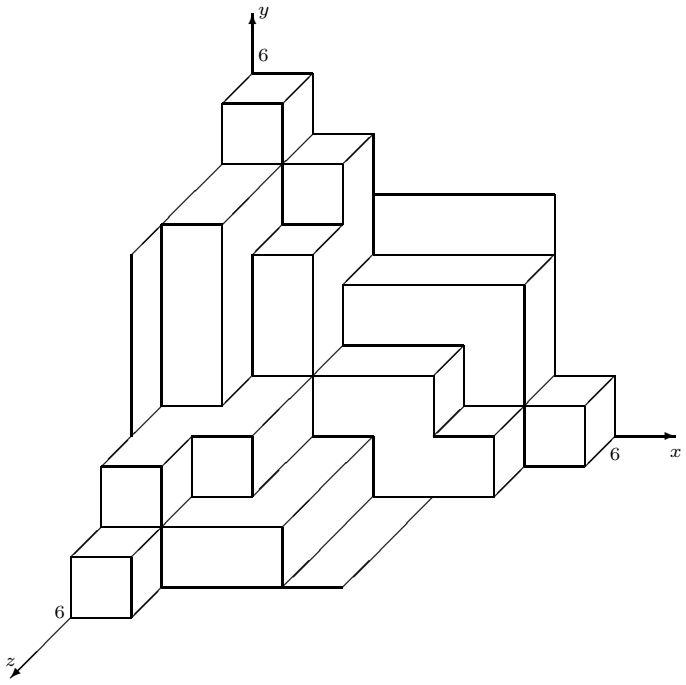

Figure 30. Example 5.10, the A-invariant ideal I

References

[1] T. P. Berger, *Automorphism groups and permutation groups of affine-invariant codes*, Finite fields and applications (Glasgow, 1995), 31 – 45, London Math. Soc. Lecture Note Ser. 233, Cambridge Univ. Press, Cambridge, 1996.

[2] T. P. Berger and P. Charpin, *The permutation group of affine-invariant extended cyclic codes*, IEEE Trans. Inform. Theory **42** (1996), 2194 – 2209.

[3] T. P. Berger and P. Charpin, *The automorphism group of BCH codes and of some affine-invariant codes on an extension field*, Designs, Codes and Cryptogr. **18** (1999), 29 – 53.

[4] P. Charpin, *Codes cyclique étendus affines-invariants et antichains d'un ensemble partiellement ordonné*, Discrete Math. **80** (1990), 229 – 247.

[5] P. Charpin, *Open problems on cyclic codes*, Handbook of coding theory, Vol. I, II, 963–1063, North-Holland, Amsterdam, 1998.

[6] P. Charpin and F. Levy-Dit-Vehel, *On self-dual affine-invariant codes*, J. Combin. Theory A **67** (1994), 223-244.

[7] P. Delsarte, *On cyclic codes that are invariant under the general linear group*, IEEE Trans. Inform. Theory **16** (1970), 760 – 769.

[8] X. Hou, *Enumeration of certain affine-invariant extended cyclic codes*, J. Combin. Theory A, **110** (2005), 71 – 95.

[9] T. Kasami, S. Lin and W. W. Peterson, *Some results on cyclic codes which are invariant under the affine group and their applications*, Inform. Contr. **11** (1968), 475 – 496.

Department of Mathematics, University of South Florida, Tampa, Florida 33620
E-mail address: xhou@math.usf.edu